



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY



COVID-19 Cyber Threats (Update)

08/13/2020

Agenda



Image source: teiss.co.uk

- Cybercriminal actors continue to take advantage of the pandemic
- Malicious coronavirus apps
- Coronavirus-themed phishing continues
- APT groups targeting COVID-19 research
- Updated COVID-19 Cyber Threat Assessment and Forecast



Slides Key:



Non-Technical: managerial, strategic and high-level (general audience)



Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)



Cybercriminals Continue to Exploit Pandemic



Financially-motivated cybercriminals continue to exploit the with targets across a variety of industry verticals including:

- Finance
- **Healthcare**
- **Pharmaceutical**
- Government
- Consulting
- Manufacturing
- Education
- Technology
- Telecommunications



Image source: Panda Security

To maximize damage and financial gain, cybercriminals are shifting their targets from individuals and small businesses to major corporations, governments and critical infrastructure, which play a crucial role in responding to the outbreak, according to INTERPOL.



Malicious Contact Tracing Apps



- In June, Anomali Threat Research identified 12 malicious applications that appear to be targeting citizens of multiple countries, many of which leverage the Anubis and SpyNote Android Trojans.
- CryCryptor surfaced just a few days after the Canadian government officially announced its intention to back the development of a nationwide, voluntary tracing app called COVID Alert.
- CryCryptor ransomware was observed targeting Android users in Canada, distributed via two websites under the guise of an official COVID-19 tracing app provided by Health Canada.
- Scammers have also deployed mobile contact tracing apps meant to pose as the U.K.'s National Health Service.
- There are also privacy concerns surrounding these apps.
- Recommend verifying the legitimacy of the developers before downloading a mobile app.

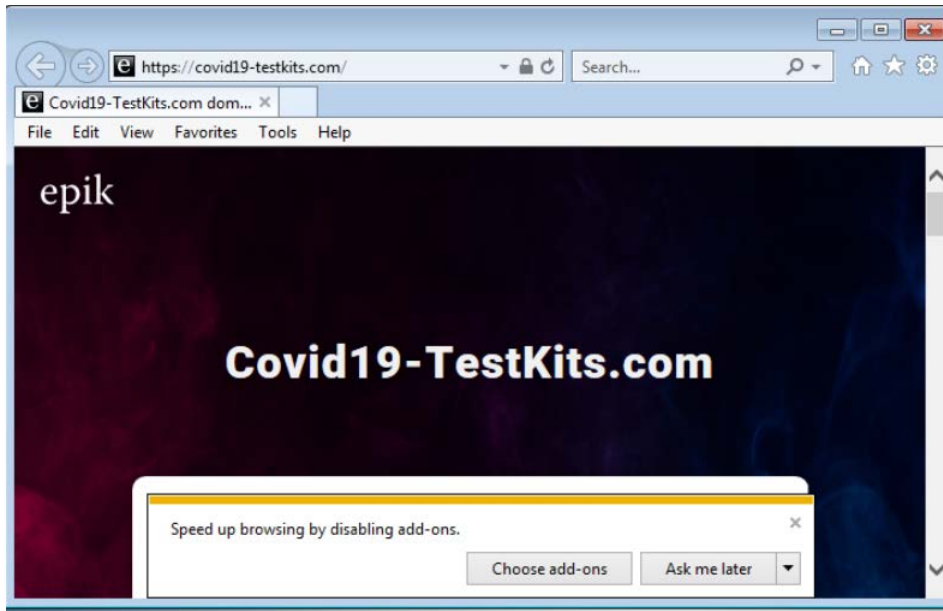
The screenshot shows a web browser window with the URL <https://tracershield.ca>. The page title is "Covid-19 Tracer App". At the top, there is a search bar with "Search Canada.ca" and a date "June, 23, 2020". The main content area features a "GET IT ON Google Play" button. Below the button, there is a message: "Download the application from our server now. The Google Play version is still under approval. Please use the latest version." A yellow button with a question mark icon says "Problems launching the app?". To the right of the button, there is text: "Let's work together to stay safe. Covid 19 Tracer App is a mobile contact tracing app that helps to let you know if you've been exposed to COVID-19 – or if you've exposed others – while protecting your privacy. Quickly identifying and isolating positive cases is an important part of our response to the COVID-19 pandemic, and preventing the spread. The more Canadians who voluntarily download and use the app, the safer we'll be, and the faster we can reopen the economy." At the bottom, there is a footer with the Canadian flag and the text "Health Canada Santé Canada". The footer also contains links for "Contact us", "Departments and agencies", "News", "Treaties, laws and regulations", "Government-wide reporting", "Prime Minister", "About government", and "Open government". The "Canada" logo is in the bottom right corner.




Coronavirus-themed Domains



- In late April to early May, almost 20,000 new coronavirus-related domains were registered, 17% of which were flagged as malicious or suspicious according to Checkpoint.
- In June, Microsoft sought legal action to seize and sinkhole a large number of COVID-19 themed domains used in a large-scale cyberattack targeting victims in 62 countries with spoofed emails in an effort to defraud unsuspecting businesses. In one week alone, the attackers sent malicious emails to millions of users, Microsoft said.
- Below is an example of a malicious coronavirus-themed domain registered in March purporting to sell COVID-19 testing kits.



MALICIOUS

 <http://www.covid19-testkits.com/>



Analyzed on: 07/31/2020 18:20:47 (UTC)

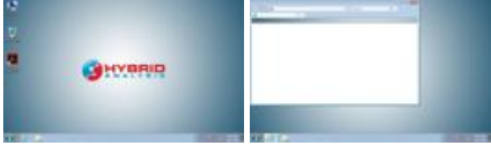
Environment: Windows 7 32 bit

Threat Score: 63/100

AV Detection: 1% Phishing site

Indicators: 2 7 14

Network:  



Coronavirus-themed Phishing



- Global COVID-19 campaigns include lures themed on regional health authority impersonations, fake vaccination information, purchase or delivery of personal protective equipment (PPE), employee targets spoofed from HR, medical and pharmaceutical supplies, and even false job promises.
- Some of the latest lures include updates on the evolution of the virus and malicious attachments that infect victims when accessed. Scammers also act under the guise of the government, leveraging the temporary ban on importing or exporting goods, or financial institutions offering COVID-19 Financial Relief.
- In late July, the FBI warned that cyber actors using Netwalker ransomware had taken advantage of the COVID-19 pandemic to compromise an increasing number of unsuspecting victims. The FBI alert notes that the operators behind Netwalker are luring victims with pandemic-themed phishing e-mails that contain an attachment with a malicious Visual Basic Scripting, or VBS, script that executes the payload once opened.



Image source: Bitdefender



Coronavirus-themed Phishing (cont.)



- A recent example of a phishing email advertising personal protective equipment (PPE) was detected by Bitdefender in July 2020.



Image source: Bitdefender



Ransomware Targeting HPH Sector



- While many ransomware operators pledged NOT to target healthcare and public health (HPH) entities during the COVID-19 pandemic, many have not followed this promise.
- In July, a healthcare company based in Maryland disclosed a NetWalker ransomware attack which took place in June and affected nearly 50,000 patients.
- Two of the most common vulnerabilities exploited by actors using Netwalker are Pulse Secure VPN (CVE-2019-11510) and Telerik UI (CVE-2019-18935).
- Maze Ransomware operators targeted a Maryland-based pharmacy in early July 2020 and a UK medical firm in March 2020.
- A US-based university paid \$1.14 million to the NetWalker ransomware operators who successfully breached its School of Medicine's IT network, stealing data and encrypting systems in early June 2020.
- Snake ransomware leaked patient data from a European healthcare conglomerate in late May 2020.
- Another campaign impersonated pharmaceutical companies to spread [F]unicorn ransomware in Italy.



Image source: Cyber Security News

Nation State Cyber Threats and Disinformation



- Iranian-linked hackers are believed to be behind an attack in early May on a US drug manufacturer which is in an advanced stage of developing a COVID-19 treatment.
- Russian APT29 and Chinese state-sponsored actors targeting organizations involved in COVID-19 vaccine development.
- These APT threat groups have engaged in disinformation campaigns surrounding the coronavirus pandemic and have targeted other countries as well with COVID-19 lures.
- 27 percent of participating countries in the Global Cybercrime Survey confirmed the circulation of false information related to COVID-19 among their communities and 21 per cent expressed a growing concern in this trend. Within a one-month period, one member country reported 290 postings and in most cases, these postings contained concealed malware.
- Additional details on disinformation campaigns can be found [here](#).

Country	Cyber Espionage	Disinformation
Iran	Yes	Yes
China	Yes	Yes
Russia	Yes	Yes





DOJ Accuses China of Targeted Hacking on COVID-19 Research Data (7 July 2020)

- In recent attacks, the hackers probed for computer network vulnerabilities of entities tasked with developing COVID-19 vaccines, testing technology, and treatments.
- Primarily exploited publicly known software vulnerabilities in popular web server software, web application development suites, and software collaboration programs
- Various techniques to compromise victims, including taking advantage of common vulnerabilities and exposures (CVEs) to target vulnerable web servers.
- Known CVEs used by these actors to gain or attempt to gain access to the victim networks include but are not limited to: CVE-2017-5638, CVE-2017-3066, CVE-2018-15961, CVE-2018-8120, CVE-2019-8394, CVE-2019-3396, CVE-2019-11510, and CVE-2019-11580.
- A significant portion of recent intrusions have used CVE-2019-11510, exploiting a vulnerability in Pulse Secure VPN. More detailed information on CVE-11510 can be found at:
<https://www.us-cert.gov/ncas/alerts/aa20-107a>.



CHINA MSS GUANGDONG STATE SECURITY DEPARTMENT HACKERS

Unauthorized Access; Conspiracy to Access Without Authorization and Damage Computers; Conspiracy to Commit Theft of Trade Secrets; Conspiracy to Commit Wire Fraud; Aggravated Identity Theft



Li Xiaoyu



Dong Jiazhi

CAUTION

On July 7, 2020, a grand jury in the United States District Court for the Eastern District of Washington indicted Li Xiaoyu and Dong Jiazhi for their alleged participation in a long-running campaign of computer network operations targeting the networks of United States and foreign companies across a wide variety of industries, including high tech manufacturing; civil, heavy, and medical device engineering; business, educational, and gaming software; solar energy; pharmaceuticals; and defense. The indictment highlighted Li and Dong's alleged actions, including a recent focus on COVID-19 research, testing, and treatment; the targeting of political dissidents, religious minorities, and human rights advocates in mainland China, Hong Kong, the United States, and Canada; and the intrusions into corporate networks of countries in Europe and Asia.

Some of Li and Dong's network operations were allegedly undertaken for their own economic benefits, while others were allegedly for the benefits of China's Ministry of State Security (MSS), including the Guangdong State Security Department.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Field Office: Seattle

www.fbi.gov

Source: fbi.gov



Russian Hackers Targeting COVID-19 Research



- According to the advisory, throughout 2020, APT29 has targeted various organizations involved in COVID-19 vaccine development in Canada, the United States and the United Kingdom, highly likely with the intention of stealing information and intellectual property relating to the development and testing of COVID-19 vaccines.
- APT29 is using custom malware known as 'WellMess' and 'WellMail' to target a number of organizations globally. This includes those organizations involved with COVID-19 vaccine development.
- WellMess and WellMail have not previously been publicly associated to APT29.
- Similar to Chinese APT actors, the group has been successful in using recently published exploits to gain initial footholds including:
 - CVE-2019-19781 (Citrix)
 - CVE-2019-11510 (Pulse Secure)
 - CVE-2018-13379 (FortiGate)
 - CVE-2019-9670 (Zimbra)



Source: Twitter

Advisory includes TTPs, IOCs, and detection & mitigation advice:

https://media.defense.gov/2020/Jul/16/2002457639/-1/-1/0/NCSC_APT29_ADVISORY-QUAD-OFFICIAL-20200709-1810.PDF



Updated COVID-19 Cyber Threat Assessment



- The percentage of COVID-19-themed phishing has remained low and relatively stable from May to early July, after declining from a peak in mid-April 2020.
- The majority of cyber espionage, information operations, and financially motivated activity leveraging COVID-19 in lures and campaigns remains consistent with established objectives, targeting patterns, and tactics, techniques, and procedures (TTPs).
- There is growing evidence of cyber espionage and financially motivated operations directly targeting organizations involved in COVID-19 response and relief efforts.
- Healthcare, pharmaceutical, government, and other related organizations face elevated near-term risk of cyber threat activity.



Projections Surrounding COVID-19 Cyber Threats



Future primary areas of concern highlighted by a recent INTERPOL [report](#) include:

- A further increase in cybercrime is highly likely in the near future.
- Vulnerabilities related to working from home and the potential for increased financial benefit will see cybercriminals continue to ramp up their activities and develop more advanced and sophisticated techniques.
- Threat actors are likely to continue proliferating coronavirus-themed online scams and phishing campaigns to leverage public concern about the pandemic.
- Business Email Compromise (BEC) schemes will also likely surge due to the economic downturn and shift in the business landscape, generating new opportunities for criminal activities.
- When a COVID-19 vaccination is available, it is highly probable that there will be another spike in phishing related to these medical products as well as network intrusion and cyberattacks to steal data.





Reference Materials



- Microsoft takes legal action against COVID-19-related cybercrime (7 July 2020)
 - <https://blogs.microsoft.com/on-the-issues/2020/07/07/digital-crimes-unit-covid-19-cybercrime/>
- Go Phish: Cybercriminals Stick to Coronavirus and Financial Content to Fuel Phishing Schemes
 - <https://hotforsecurity.bitdefender.com/blog/go-phish-cybercriminals-stick-to-coronavirus-and-financial-content-to-fuel-phishing-schemes-23708.html>
- Threat Actors Adapt to the Pandemic by Unleashing New Phishing Trends
 - <https://cyware.com/news/threat-actors-adapt-to-the-pandemic-by-unleashing-new-phishing-trends-72c73a7f>
- Protecting businesses against cyber threats during COVID-19 and beyond (16 April 2020)
 - <https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond>
- Microsoft secretly seized domains used in COVID-19-themed email cyberattacks (7 July 2020)
 - <https://techcrunch.com/2020/07/07/microsoft-domains-covid-19-attacks/>
- Coronavirus phishing emails: How to protect against COVID-19 scams
 - <https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html>
- Coronavirus cyber-attacks update: beware of the phish
 - <https://blog.checkpoint.com/2020/05/12/coronavirus-cyber-attacks-update-beware-of-the-phish/>
- Here's a list of all the ransomware gangs who will steal and leak your data if you don't pay (21 April 2020)
 - <https://www.zdnet.com/article/heres-a-list-of-all-the-ransomware-gangs-who-will-steal-and-leak-your-data-if-you-dont-pay/>
- FBI: COVID-19-Themed Phishing Spreads Netwalker Ransomware (31 July 2020)
 - <https://www.bankinfosecurity.com/fbi-covid-19-themed-phishing-spreads-netwalker-ransomware-a-14744>



- INTERPOL report shows alarming rate of cyberattacks during COVID-19 (4 August 2020)
 - <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>
- Department of Justice, Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research
 - <https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion>
- Virginia becomes first US state to debut COVID-19 tracing app using Apple and Google API
 - <https://9to5mac.com/2020/08/05/virginia-becomes-first-us-state-to-debut-covid-19-tracing-app-using-apple-and-google-api/>
- Google said it took down ten influence operation campaigns in Q2 2020 (6 August 2020)
 - <https://www.zdnet.com/article/google-discloses-new-takedowns-of-influence-ops-on-its-sites/>
- NSA Teams with NCSC, CSE, DHS CISA to Expose Russian Intelligence Services Targeting COVID-19 Researchers
 - www.nsa.gov/news-features/press-room/Article/2275378/nsa-teams-with-ncsc-cse-dhs-cisa-to-expose-russian-intelligence-services-target
- Exclusive: Iran-linked hackers recently targeted coronavirus drugmaker Gilead – sources (8 May 2020)
 - <https://www.reuters.com/article/us-healthcare-coronavirus-gilead-iran-ex/exclusive-iran-linked-hackers-recently-targeted-coronavirus-drugmaker-gilead-sources-idUSKBN22K2EV>
- Anomali Threat Research Identifies Fake COVID-19 Contact Tracing Apps Used to Download Malware that Monitors Devices, Steals Personal Data (10 June 2020)
 - www.anomali.com/blog/anomali-threat-research-identifies-fake-covid-19-contact-tracing-apps-used-to-monitor-devices-steal-personal-data



Questions



Upcoming Briefs

- 5G Security (Update) (8/20)
- Pulse Secure VPN Vulnerability and Incident Case Study (8/27)
- CIS 20 Controls and HPH (9/3)

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.



HC3 Customer
Feedback

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110**.

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.



HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products



Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG



White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.



Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Visit us at: www.HHS.Gov/HC3



Contact



www.HHS.GOV/HC3



(202) 691-2110



HC3@HHS.GOV