LAC-CSIRTs
May 08, 2020
Online Event
Incident Handling Amid a Pandemic: Now What?

Dr. Cristine Hoepers
General Manager
cristine@cert.br
Creation:

**August/1996**: a report proposing a model for incident management for the country is published by the Brazilian Internet Steering Committee – CGI.br

**June/1997**: CGI.br creates CERT.br (at that time called NBSO – NIC BR Security Office) based on the report’s recommendations

---

**Mission**

To increase the level of security and incident handling capacity of the networks connected to the Internet in Brazil.

**Constituency**

Networks that use Internet Resources allocated by NIC.br (IPs or ASNs allocated to Brazil, and domains under the ccTLD .br)

**Focus of the Activities**

- National focal point for incident reports
- Support technical analysis and the understanding of attacks and threats
- Develop collaborative relationships with other entities
- Increase incident detection, event correlation and trend analysis in the country
- Transfer knowledge through courses, best practices and awareness materials

---

**Filiations and Partnerships:**

- First
- Trusted Introducer
- APWG Research Partner
- SEI Partner Network
- Antiphishing.org
- HN/P

---

1. [https://www.nic.br/grupo/historico-gts.htm](https://www.nic.br/grupo/historico-gts.htm)
2. [https://www.nic.br/pagina/gts/157](https://www.nic.br/pagina/gts/157)
Join us in sharing pandemic related cyber threat intelligence during this time of crisis.

Roundup: COVID-19 pandemic delivers extraordinary array of cybersecurity challenges

As the COVID-19 outbreak threatens to overload the healthcare system and also having a powerful impact on the security of systems.

MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing

COVID-19 MISP Information Sharing Community
COVID-19 MISP is a MISP instance retrofitted for a COVID-19 information sharing community, focusing on two areas of sharing:

Table of Content
- COVID-19 MISP Information Sharing Community
Phishing Statistics

Top graphic includes:
- Total reports
- COVID-19 themed phishing reports
- Top 5 brands (e002, e004, e010, e014 and e023)

Bottom graphic includes:
- Total reports
- COVID-19 themed phishing reports
Another type of problem: Fake News and Scams

Usually spread through social networks and messaging apps
- Facebook, Instagram, Twitter, WhatsApp, Telegram, etc

Underreported
- hard to detect
  - unless you are the owner of the platform
- hard to report
  - specially to CSIRTs
The road to hell is paved with good intentions...

**MISP covid instance blacklist**
(covid_misp_filtered_ioc_list.csv)

- entries: 168,778
- .br domains: 624
- legit.gov.br domains: 60

- additionally, at least:
  - 8 legit telemedicine sites
  - 20 university covid-19 info pages

- other .br domains blacklisted include covid-19 information hot sites of hospitals and news outlets

**This should make us think**

How many people where prevented from getting help and access important information?

- The lists are basically a `grep` for anything that matches `covid` or `corona` in
  - passive DNS collectors
  - lists of newly generated domains

- Plus lots of other domains not related to COVID, like “regular” phishing (banks, ecommerce, etc)
  - how this affects the numbers being shouted in the media?

- No human validation
- No easy way to provide feedback

Source: [https://www.misp-project.org/covid-19-misp/](https://www.misp-project.org/covid-19-misp/)
Lessons Learned

Continue normal operations
– The types of incidents are not likely to change
  – current/extreme events will be used as a lure
  – this has happened before
    • earthquakes, Olympics, tsunamis, etc
– Exposure is likely to change due to unplanned remote working (but nothing really new)
  – internal services exposed
  – less control over desktops/laptops security
  – use of new tools with no training
– Don’t panic
  – even if others are panicking
  – don’t be too quick to block everything and blacklist everyone

Always be prepared
– to work remotely securely
  – equipment and tools
  – multi-factor authentication
– to share information
  – participate in task forces
  – use information sharing platforms
– to provide high level information
  – statistics, briefings, reports, etc
– to educate your constituency!
  – have well known channels
  – enlist the help of others
Edição Especial COVID-19

Infelizmente, em momentos de incerteza e de busca por informações como os que estamos vivendo com a pandemia do Coronavirus, algumas pessoas se aproveitam para aplicar golpes e espalhar notícias falsas.

Por isso é importante que você adote na Internet a mesma postura preventiva que vem adotando para se proteger do Coronavirus. Para ajudá-lo nisso preparamos algumas dicas:

- Boatos ajudam a espalhar desinformação pela Internet e podem conter códigos maliciosos e tentativas de golpes. Ao receber notícias sobre o tema Coronavirus seja cuidadoso ao compartilhar, verifique a fonte da informação e em caso de dúvidas, não compartilhe e ajude a tornar a Internet um ambiente mais saudável, seguro e confiável.

- Caso tenha dúvidas sobre a veracidade de uma informação, como por exemplo um remédio milagroso, procure consultar outras fontes antes de repassá-la.

- Cuidado com mensagens solicitando doações para as vítimas da doença. Apesar de existirem várias ações reais a respeito, muitos golpistas exploram a propensão à caridade que as pessoas demonstram em momentos difíceis como estes para criar campanhas falsas. Antes de doar procure obter mais informações consultando os sites oficiais de Campanhas.

- Caso perceba pessoas em seus grupos compartilhando mensagens com suspeitas de golpes, alerte-os sobre o conteúdo malicioso.

- Cuidado com mensagens que tentem induzi-lo a fornecer informações pessoais e dados bancários, como páginas que prometem fazer testes on-line para verificar se você está infectado, mas que solicitam os números do seu cartão de crédito.

- Tenha cuidado ao instalar aplicativos que prometem informações sobre a pandemia, procure baixá-los de desenvolvedores e lojas oficiais, como o do sistema operacional do seu aparelho. Ao instalar aplicativos, evite fornecer dados e permissões quando não forem realmente necessários.
Thank You

@ cristine@cert.br

@ Incident reports to: cert@cert.br  @ certbr

https://cert.br/

May 08, 2020

nic.br  cgi.br
www.nic.br | www.cgi.br