Cyber Security Bulletin

2020 - 49 **11 March 2020**

Cyber Security Center

Email:
SAICCyber@dps.ohio.gov

Tip Line:
(614) 387-0447

Executive Director:
Brian L. Quinn

The purpose of this document is to provide a summary and information regarding cyber security and the Coronavirus, also known as COVID-19.

Cyber Security Advisory

Cyber threat actors are exploiting the Coronavirus scare with different types of attacks towards individuals and organizations.

Executive Summary

The Cybersecurity and Infrastructure Agency (CISA) recently issued a document outlining the possibility that cyber threat actors may exploit the Coronavirus scare. In the past, cyber actors have been observed using public health threats and other high-profile events to reach out and trick victims into providing personally identifiable information or downloading malware onto their machine.

Details

Who is Targeted?

The Multi State Information Sharing and Analysis Center (MS-ISAC) have observed dedicated attacks against construction, education, energy, healthcare, industry, manufacturing, retail, and transportation companies[1]. Workers in insurance, healthcare and the pharmaceutical industry throughout the world are common targets for malicious cyber actors[2].

Keywords

As of February 1, 2020, MS-ISAC has observed the registration of domain names containing the phrase “coronavirus.” The majority of these new domains include a combination of the words “help,” “relief,” “victims,” and “recover[1].”

Cyber Security Bulletin

2020 - 49

11 March 2020

Cyber Security Center

Email:
SAICCyber@dps.ohio.gov

Tip Line:
(614) 387-0447

Executive Director:
Brian L. Quinn

Misinformation/Disinformation

The potential of misinformation during times of high-profile global events and public health threats is high and users should verify information before trusting or reacting to posts on social media. Malicious actors often use social media to post false information or links to malicious websites. The MS-ISAC observed similar tactics in the days following Hurricane Irma's landfall and other natural disasters[1].

Phishing Emails

Cyber threat actors may also capitalize on outbreaks by sending phishing emails with links to malicious websites advertising information that appears relevant to the outbreak[1]. The websites may contain malware or links to fraudulent websites that request login credentials. Other malicious spam will likely contain links to, or attachments with, embedded malware. Victims who click on links or open malicious attachments risk compromising their computer to malicious actors. Cybercriminals were already using convincing but fake emails from the World Health Organization (WHO), the Center for Disease Control (CDC), and Japanese government to trick people into downloading PDF, MP4, and Microsoft Word DOCX files[3]. Some emails were observed leveraging malicious Word attachments with AZORult malware, an information-stealer based malware. Stolen emails from previously compromised accounts are being exploited as templates to further spread malicious infections (spoofing)[4]. Two cyber security firms discovered an Emotet campaign delivered using Coronavirus themed phishing attempts. Analysis validated that none of the identified samples were new, but were reused with some small changes[4]. Two Coronavirus themed Android mobile applications have been identified:

- Coronavirus[.]apk
- Coronavirus[.]hijosdept[.]cacaic

Cyber Security Bulletin

2020 - 49 **11 March 2020**

Cyber Security Center

Email:
SAICCyber@dps.ohio.gov

Tip Line:
(614) 387-0447

Executive Director:
Brian L. Quinn

Malware

Researchers at the enterprise security company ProofPoint(USBUS) discovered indicators that hackers were spoofing a top U.S. medical center and sending fake HIV test results to victims via email[2]. The Koadic malware found in these emails gives hackers access to a computer and the victim's data, including sensitive personal and financial information[2].

References

[1] https://www.cisecurity.org/newsletter/cyber-threat-actors-expected-to-leverage-coronavirus-outbreak/

[2] https://www.fiercehealthcare.com/tech/hackers-using-fake-hiv-test-results-coronavirus-emails-to-target-healthcare-companies

[3] https://www.techrepublic.com/article/cybercriminals-flooding-web-with-coronavirus-themed-spam-and-malware/

[4] Cybersecurity and Infrastructure Security Agency Integrated Operations Division. 3 March 2020. Situation Report. COVID-19 – Worldwide – 03-05-20 (Update 5) | (INC10276272).

For any questions on this product, please contact the Ohio Homeland Security Cyber Center at (614) 387-0447 or by email at SAICCyber@dps.ohio.gov.

Please report any suspicious activity to at (877) OHS-INTEL (647-4683) or to STACC@dps.ohio.gov.