Healthcare and Cross-Sector Cybersecurity Report

www.himss.org/cyberreport

Volume 33 – April 2020

Authored by: Lee Kim, BS, JD, CISSP, CIPP/US, FHIMSS

Threat, Vulnerability, and Mitigation Information

1. Cybercriminals, state-sponsored actors, and others are now investing significant effort and time with COVID-19 phishing campaigns using means such as text messages, e-mails, social media messages, phishing websites, and advertisements. Both consumers and businesses of all types are targets. The objective of these phishing campaigns vary, such as money (business e-mail compromise and ransomware), crippling of systems (ransomware and distributed denial of service attacks), credential stealing (including in regard to email accounts and popular web conferencing platforms), and more.

   While phishing remains a significant threat during the COVID-19 pandemic, criminals are also heavily engaged in financial fraud (including in regard to economic stimulus payments), intellectual property theft, distributed denial of service campaigns, and more. In summary, criminals are capitalizing on current events and are preying on fear and concern of individuals with respect to the COVID-19 pandemic.

2. Hospitals, government agencies, and others are experiencing distributed denial of service attacks (some successful and attempts in other cases). In the case of successful attacks, some organizations have had to completely shut down their network according to reports.

3. Multiple ransomware campaigns have been active at least since early April according to researchers. Vulnerable remote desktop protocol servers (such as those that may be vulnerable to brute force attacks and without multi-factor authentication), virtual private network ("VPN") systems, virtual desktop endpoints and other virtual environments (such as those that do not have multi-factor authentication implemented), legacy operating systems, and devices exposed to the Internet have been targeted by cybercriminals. Additional information on cyber-attacks that target remote work tools like as remote desktop protocol may be found here.

4. INTERPOL and Europol have issued warnings to hospitals and other organizations involving in the global response to the COVID-19 pandemic that they are now targets for ransomware attacks in an effort for criminals to extort payments from the victim organizations.

5. Significant security incidents have led to some hospitals reportedly postponing urgent surgical interventions and rerouting new patients to nearby hospitals. Healthcare organizations are thought to have been the target of aggressive cyber-attack due to COVID-19 related treatment of patients, lab testing services, vaccine testing services, and/or biosafety labs.

6. Blocklists are available for COVID-19 vetted (verified suspicious as per coalition analysts) and unvetted (as yet unconfirmed suspicious as per coalition analysts) data sets, including domain names and uniform resource locators (URLs).

Research and reports

1. With a good number of workforce members now working from home due to the COVID-19 pandemic, some survey respondents have reported an uptick in security incidents and cybercrime. Additionally, some survey respondents have reported spending more time in IT support roles instead of their usual cybersecurity rules. Finally, while best practices are being adhered to, many respondents admitted that more can be done in that vein.

2. With many physicians and others working from home during the COVID-19 pandemic, associations and other entities have released guidance on cybersecurity awareness. These include medical associations, veterinary associations, state government agencies (with an alert addressed to medical professionals), cybersecurity professional associations, financial industry associations, and others.

3. Researchers have provided an in-depth look on how advanced persistent threat actors use the COVID-19 as a lure in their campaigns. Remote access trojans, banking trojans (such as Dridex), botnets (such as Emotet), and other types of malware (such as malicious LNK files) are used to persist on networks by infecting the machines of victims. Malware analysis of a remote access trojan that runs on the Java platform may be found here.

4. Criminal groups have reorganized themselves to take advantage of the COVID-19 pandemic. Law enforcement related agencies across the glove have reported significant amounts of **fake** medical items (such as anti-flu and anti-viral preparations), testing kits, vaccines, preventive masks, sanitizers, and antiseptic solutions. By expertly leveraging search engine optimization ("SEO"), the websites and applications set up by these criminals bubble up to the top. Thus, innocent victims may fall victim and, as a result may unwittingly disclose sensitive information such as banking information.

5. Reports have also surfaced in terms of **fake** calls from (purportedly) nearby hospitals where loved ones may be hospitalized in order to obtain online payments from innocent victims (such criminals learn of these facts about the victims through social media).

7. Resources are available for consumers (such as from state attorneys general), for businesses (including for those in the financial sector such as card network providers and payment card industry standards bodies), and from the government to bolster security awareness and help guard against criminal activity during the COVID-19 pandemic.

Special Announcements

1. Join the HIMSS Healthcare Cybersecurity Community today! The HIMSS Healthcare Cybersecurity Community provides a monthly forum for thought-leaders and healthcare constituents to discuss and learn about advancing the state of cybersecurity in the healthcare sector. Please note: HIMSS membership is required to join the HIMSS Healthcare Cybersecurity Community.

2. Take the 2020 HIMSS Cybersecurity Survey today! Let's hear your voice. Your opinion matters.