American Technology Services
a WWTS Company

2020-01 ATS Security Advisory

COVID-19 Phishing Scheme Targeting Remote Workers

Summary

In light of the heightened fear around the COVID-19 pandemic, criminals are targeting and exploiting remote workers that are isolated from their regular daily routines. This week the U.S. Secret Service issued an alert around coronavirus-related phishing scams.

"Cybercriminals are exploiting the coronavirus through the wide distribution of mass emails posing as legitimate medical and or health organizations," the guidance reads. "In one particular instance, victims have received an email purporting to be from a medical/health organization that included attachments supposedly containing pertinent information regarding the Coronavirus. This led to either unsuspecting victims opening the attachment, causing malware to infect their system, or prompting the victim to enter their email login credentials to access the information resulting in harvested login credentials."

Another emerging fraud scheme exploiting the Coronavirus is using social engineering tactics through legitimate social media websites seeking donations for charitable causes related to the virus. Criminals are exploiting the charitable spirit of individuals, seeking donations to fraudulent causes surrounding the Coronavirus. Increased caution should be exercised when donating to charitable organizations.
Lindsay Kaye, director of operation outcomes at Recorded Future specifically called out the following domains as potentially dangerous:

- coronavirusstatus[.]space
- coronavirus-map[.]com
- blogcoronacl.canalcero[.]digital
- Coronavirus [.]zone
- coronavirus-realtime[.]com
- Coronavirus [.]app
- bgvfr.coronavirusaware[.]xyz
- coronavirusaware[.]xyz

2020-01 ATS Security Advisory

What Can You Do?

- **Phishing Emails / Social Engineering** – Avoid opening attachments and clicking on links within emails from senders you do not recognize. These attachments can contain malicious content, such as ransomware, that can infect your device and steal your information. Be suspicious of emails or phone calls requesting account information or requesting you to verify your account. Legitimate businesses will never call you or email you directly for this information.
- Always independently verify any requested information originates from a legitimate source.
- Visit websites by inputting the domain name yourself. Business use encryption, Secure Socket Layer (SSL). Certificate "errors" can be a warning sign that something is not right with the website.

If you suspect that an email is malicious, please forward the email to helpdesk@networkats.com so that we may investigate further.

References:

[0] https://www.secretservice.gov/press/releases/
[1] https://www.recordedfuture.com/
[2] https://www.forbes.com/sites/thomasbrewster/2020/03/12/coronavirus-scam-alert-watch-out-for-these-risky-covid-19-websites-and-emails/#42d7c9b01099