Formbook Malware Phishing Campaigns

Executive Summary

On May 20, 2020, researchers reported an increase of Formbook malware phishing campaigns using COVID-19 themes from May 6 to May 20. This recent campaign targeted educational institutions; in April, however, Formbook targeted "biomedical firms, compromising financial resources, data, or intellectual property." On April 16, FireEye reported that Formbook made up about 8% of their top malware detections in the healthcare industry in Q1 2020. The malware Ursnif and Emotet combined made up over 65% of their detections. The Cybersecurity and Infrastructure Security Agency (CISA) identified Formbook, associated with CVE-2017-11882, as a "top 10 most exploited vulnerabilities by state, [non-state], and unattributed cyber actors from 2016 to 2019." CISA recommends updating affected Microsoft products with the latest security patches. Patching CVE-2017-11882 will significantly reduce the threat posed by Formbook to an organization given the frequent targeting of the vulnerability by various cyber threat actors.

Report

Researchers at SentinelLabs reported an increase of Formbook malware phishing campaigns using COVID-19 themes from May 6 to May 20. This recent campaign targeted "educational institutions, via phishing messages, with a trojanized application for teachers." However, in April, Formbook targeted "biomedical firms, compromising financial resources, data, or intellectual property." Since early February 2020, Formbook cyber threat actors used COVID-19-themed phishing emails appearing to be from the World Health Organization (WHO) to lure their victims.

Used since 2016, Formbook is an information stealing malware, also known as "form grabber" malware. The malware is installed on victims' computers when they visit malicious websites or domains. Form grabber malware primarily targets login credentials and other valuable information on web forms that are often banking related. The malware can "circumvent HTTPS encryption and intercept data before it is even transmitted" to include auto-fill and clipboard-stored data as well as, "input from virtual keyboards."

On April 16, FireEye reported that Formbook made up about 8% of their top malware detections in the healthcare industry in Q1 2020. The malware Ursnif and Emotet combined made up over 65% of their detections. CISA identified Formbook, associated with CVE-2017-11882, as a "top 10 most exploited vulnerabilities by state, [non-state], and unattributed cyber actors from 2016 to 2019." This vulnerability affects Microsoft Office 2007 SP3/2010 SP2/2013 SP1/2016 products. **CISA recommends updating affected Microsoft products with the latest security patches.**

References

Walter, Jim. “Threat Intel: Cyber Attacks Leveraging the COVID-19/CoronaVirus Pandemic,” May 28, 2020. https://labs.sentinelone.com/threat-intel-update-cyber-attacks-leveraging-the-covid-19-coronavirus-pandemic/.

Yedakula, Kalyan. “Formbook Campaign Now Leveraging COVID-19 Themes: Cyware Hacker News,” April 28, 2020. https://cyware.com/news/formbook-campaign-now-leveraging-covid-19-themes-92325530.

O'Conner, Melchezadec. “Form Grabber: Definition of Form Grabber by Malware.xyz,” April 4, 2020. https://malware.xyz/glossary/form-grabber.

“Alert (AA20-133A): Top 10 Routinely Exploited Vulnerabilities,” n.d. https://www.us-cert.gov/ncas/alerts/aa20-133a.