Security Brief

COVID19-Themed Malware and Cyber-Attacks – Overview & Protection Measures

Dor Cohen

Senior Cyber Security Researcher, Radiflow

radiflow

COVID19-THEMED MALWARE AND CYBER-ATTACKS – OVERVIEW & PROTECTION MEASURES

To help our customers protect their networks during this global event, we at Radiflow have created a new Snort rule-set consisted of known threat actors that have been exploiting COVID-19-related threats.

Radiflow now also offers a 90-day trial of iSID to help OT operators protect their networks during the COVID19 outbreak.

As COVID-19 spreads around the world, threat actors have been launching malware COVID-19-themed malware campaigns and cyber attacks that take advantage of people's interest and need for information related to the disease.

According to Trend Micro over 80,000 and 45,000 spam and malware attacks took place in the UK and in France respectively. Europe is a leader in the number of attacks, followed by Asia, North America, and Latin America.

Here's a very partial list of findings:

- **Attacks exploiting fears and thirst for information:** this includes websites selling medical products, fake news stories, phishing campaigns, and social engineering. Many hackers publish advertisements for deals and discounts on COVID-19-related products.
- **Targeting hospitals and health centers**: we have noticed on hacker forums that hackers have been targeting facilities and organizations related to COVID-19. Interestingly, some hacker groups have publicly committed to avoid targeting hospitals and health centers. An especially creative hacker group used one of its victims' website to publish a fake "press release", stating that "due to situation with incoming global economy crisis and virus pandemic it would be offering discounts to victims of their ransomware."
- **Attackers use a new CoronaVirus Ransomware as a cover for Kpot Infostealer infections:** security experts from MalwareHunterTeam detected new ransomware dubbed CoronaVirus has been distributed through a malicious web site that was advertising a legitimate system optimization software and utilities from WiseCleaner.
- **Coronavirus news used by Emotet and Trickbot to evade detection:** Experts warn of new Coronavirus-themed attacks that are spreading TrickBot and Emotet (a banking Trojan that has evolved into a full-service threat-delivery mechanism which can install a malware package including information stealers, email harvesters, self-propagation mechanisms and ransomware). Researchers from BleepingComputer discovered that the crypters for TrickBot and Emotet have started using news stories about the Coronavirus outbreak (Crypters are software used to encrypt, obfuscate, and manipulate malware, to evade detection of solutions that employ machine-learning or artificial intelligence.)
- **New Coronavirus-themed attack uses fake WHO chief emails -** Experts from IBM X-Force have uncovered a new Coronavirus-themed phishing campaign aimed at delivering keyloggers on users' PCs. Threat actors are using phishing emails claiming to have been sent by the chief of the World Health Organization (WHO). This malware is a new variant of HawkEye keylogger, which was designed to steal credentials from applications but has been observed to also also include "loader" capabilities.
- **APT27 joins the fray:** Security researcher Marco Ramilli analyzed a new COVID-19-themed attack gathering evidence of the alleged involvement of the APT27 group.

RECOMMENDATIONS FOR RADIFLOW CLIENTS:

- If you monitor network traffic using a SPAN (Port Mirroring) or TAP, using iSID, search for instances of COVID-19 related threats (e.g. spearphishing, Emotet malware, Trickbot malware) on your network. iSID uses IDS ruleset updates from multiple threat intelligence providers as well as Radiflow's own research. These rulesets include COVID-19-related threats signatures, which monitor your incoming traffic for known COVID-19-related threats characteristics. The latest rules package also include Crimson RAT, Calyx TOR anonymizer device, Generic IcedID, PlugX, Citrix ADC exploit and more.
- Remote Access management:
    - Use iSID to monitor all external connections.
    - Privileged users such as domain administrators should maintain separate accounts and be prohibited from remote access using their privileged credentials. These privileged users should escalate access when necessary on their OT network. Access control policies should reflect a layered network defense model (e.g. the Purdue model) to mitigate lateral movement in the event of a compromise and protect the most sensitive and critical process control assets.
    - Authentication: industrial organizations should implement MFA on all external corporate resources to reduce the ability of network and application access through credential spraying, password stuffing and phishing attacks.

- Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services.

- Consider using this time to test Radiflow's iRISK risk assessment service. iRISK automatically generates a comprehensive risk-status report, detailing network properties, overall risk score, extent of risk introduced by devices and protocols, likelihood of lateral threat movement between business processes, potential attack paths and more. In addition, iRISK provides applicable ISO/IEC 62443-compliant remediation recommendations, specifying which corrective actions improve the network's security posture.

Radiflow continuously monitors various data feeds from leading ICS vendors and system integrators (e.g. Siemens, Schneider Electric, Rockwell Automation) to provide timely notification of security vulnerabilities and advisories and to incorporate this knowledge in Radiflow's solutions.

Finally, we recommend that you read the following advisories:

- https://coronavirusphishing.com/
- https://www.cisa.gov/coronavirus
- https://www.enisa.europa.eu/news/enisa-news/joint-fight-against-covid-19-related-threats

For more information on how to protect your industrial network and assets, please contact us.

ABOUT RADIFLOW

Radiflow is a leading provider of industrial cyber security solutions for critical business operations. Our comprehensive portfolio of cybersecurity solutions empowers critical infrastructure and industrial enterprises to maintain visibility, control and security of their operational environment. Our intelligent threat management for Industrial cybersecurity minimizes potential business interruption and loss within your OT environment. The Radiflow team consists of professionals from diverse backgrounds, from veterans of military cyber and communications units to former employees of leading players in the industry. Founded in 2009, Radiflow' first solutions were launched in late 2011, validated by leading research labs and successfully deployed by major utilities worldwide. More at www.radiflow.com.