EG & IT Division

CYBER SECURITY AWARENESS NEWSLETTER

For internal distribution

Vol :1/ Issue No:01 /18 March 2020

“Careless clicking on links and downloading of malicious email attachments may end up with data theft or loss of credentials”

Signs of Infection

Executing the Corona-virus-Map.com.exe results in the creation of duplicates of the Corona-virus-Map.com.exe file and multiple Corona.exe, Bin.exe, Build.exe, and Windows.Globalization.Fontgroups.exe files

Technical details upon studying the malware,

The malware is embedded in the file, usually named as *Corona-virus-Map.com.exe*. It's a small Win32 EXE file with a payload size of only around 3.26 MB. Double-clicking the file opens a window that shows various information about the spread of COVID-19. The centerpiece is a "map of infections" similar to the one hosted by **Johns Hopkins University**, a **legitimate online source** to visualize and track reported coronavirus cases in the real-time. Numbers of confirmed cases in different countries are presented on the left side while stats on deaths and recoveries are on the right. The window appears to be interactive, with tabs for various other related information and links to sources. It presents a convincing GUI not many would suspect to be harmful. The information presented is not an amalgamation of random data, instead is actual COVID-19 information pooled from the Johns Hopkins website.

Beware of 'Coronavirus Maps' – It's a malware infecting PCs to steal passwords

Cyber criminals will leave no opportunity to exploit every chance to prey on internet users. Even the disastrous spread of SARS-COV-II (the virus), which causes COVID-19 (the disease), is becoming an opportunity for them to likewise spread malware or launch cyber attacks. Reason Cybersecurity recently released a threat analysis report detailing a new attack that takes advantage of internet users' increased craving for information about the novel coronavirus that is wreaking havoc worldwide. The malware attack specifically aims to target those who are looking for cartographic presentations of the spread of COVID-19 on the Internet, and tricks them to download and run a malicious application that, on its front-end, shows a map loaded from a legit online source but in the background compromises the computer. New Threat With An Old Malware Component The latest threat, designed to steal information from unwitting victims, has vicitimised many innocent users so far.

It involves a malware identified as AZORult, an information-stealing malicious software discovered in 2016. AZORult malware collects information stored in web browsers, particularly cookies, browsing histories, user IDs, passwords, and even cryptocurrency keys.

EG & IT Division

CYBER SECURITY AWARENESS NEWSLETTER

For internal distribution

Vol :1/ Issue No:01 /18 March 2020

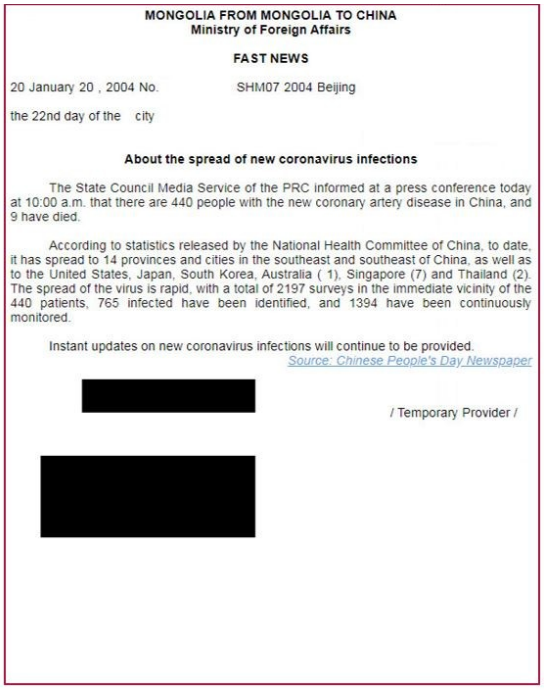
The APT group was spotted sending spear-phishing emails that purport to detail information about coronavirus – but they actually infect victims with a custom Remote Access Trojan(RAT)

An Advanced Persistent Threat (APT) group is leveraging the coronavirus pandemic to infect victims with a previously unknown malware, in a recently discovered campaign that researchers call “Vicious Panda.”

Researchers identified two suspicious Rich Text Format files (RTF — a text file format used by Microsoft products) targeting the Mongolian public sector. Once opened, a custom and unique remote-access trojan (RAT) is executed that takes screenshots of the device, develops a list of files and directories, downloads files and more.

This specific campaign leverages the COVID-19 pandemic to lure victims to trigger the infection chain.” The emails allege to be from the Mongolian Ministry of Foreign Affairs, and claim to inform victims about the prevalence of new coronavirus infections. The RTF files attached to the email were actually weaponized using a version of a tool named *RoyalRoad.* This tool, commonly used by various Chinese threat actors, allows the attacker to create customized documents with embedded objects that exploit unspecified vulnerabilities in Equation Editor, a tool for building complex equations in Microsoft Word After the victim opens the specially crafted RTF document, and the Microsoft Word vulnerability is exploited, a malicious file (intel.wll) is dropped into the Microsoft Word startup folder *(%APPDATA %\Microsoft\Word\STARTUP).* The file, intel.wll, then downloads a DLL file, which serves as the loader for the malware, and which also communicates with the threat actor’s command-and-control (C2) server.

When looking at attribution, researchers compared the campaign to one from 2017 where threat actors were targeting the government of Belarus using the CMSTAR trojan. Researchers said they found infrastructure and code similarities in the payload between the two campaigns. It also seems to have links to other operations which were carried out by the same anonymous group, dating back to at least 2016. Over the years, these operations targeted different sectors in multiple countries, such as Ukraine, Russia and Belarus.



MONGOLIA FROM MONGOLIA TO CHINA
Ministry of Foreign Affairs

FAST NEWS

20 January 20 , 2004 No. SHM07 2004 Beijing

the 22nd day of the city

About the spread of new coronavirus infections

The State Council Media Service of the PRC informed at a press conference today at 10:00 a.m. that there are 440 people with the new coronary artery disease in China, and 9 have died.

According to statistics released by the National Health Committee of China, to date, it has spread to 14 provinces and cities in the southeast and southeast of China, as well as to the United States, Japan, South Korea, Australia (1), Singapore (7) and Thailand (2). The spread of the virus is rapid, with a total of 2197 surveys in the immediate vicinity of the 440 patients, 765 infected have been identified, and 1394 have been continuously monitored.

Instant updates on new coronavirus infections will continue to be provided.

Source: Chinese People's Day Newspaper

[redacted]

/ Temporary Provider /

[redacted]

Translated Email Snapshot

DISCLAIMER:

The information published in this document has been compiled from various open sources, solely for the purpose of spreading awareness. The issuing agency is not the author of these contents.

Dr S. Janakiraman

JS(EG&IT)