RISKIQ®

RISKIQ I3 INTELLIGENCE BRIEF:

Ransomware Attacks the Next Consequence of the Coronavirus Outbreak

March 3, 2020
Team RiskIQ

Summary:

As the coronavirus continues to spread around the globe, RiskIQ assesses with a moderate-high level of confidence that cybercriminals will leverage the global anxiety surrounding the coronavirus outbreak to execute ransomware attacks. We believe these attacks will focus on corporations because most rely heavily on markets and supply chains originating in China and other affected regions. Therefore, they will be laser-focused on the developments related to the virus.

Secondary targets could include health organizations involved in tracking the spread, finding a cure, or providing associated public service functions. Targets of opportunity could consist of any institution or individual seeking general information about the spread and impact of the virus.

We assess that there are two likely methods of attack; both include phishing campaigns. The first involves the AZORult malware, which attackers used to deploy ransomware on at least three different occasions since 2018. In January 2020, researchers witnessed an AZORult-based phishing campaign targeting members of the shipping industry, who would have considerable interest in the effect the virus might have on their operations. In this case, there is no evidence yet that ransomware was actually deployed.

The second phishing campaign relies on the Emotet Trojan. Victims in Japan have received emails claiming to contain important information about the coronavirus, but clicking on the link activates Emotet. As with AZORult, we have not yet seen the coronavirus scheme used to deploy ransomware via Emotet. However, in September 2019, criminals did just that in an unrelated malware campaign, partnering Emotet with TrikBot and Ryuk ransomware.

Given these recent successes of deploying ransomware via AZORult and Emotet, RiskIQ assesses that it's only a matter of time before cybercriminals return to this methodology. Coronavirus is an ideal opportunity.

Background

In late 2019, word began to emerge of a deadly virus spreading through the Chinese city of Wuhan. On January 30, 2020, the World Health Organization (WHO) declared a public health emergency of international concern (or PHEIC) in response to the outbreak. By the end of February, the WHO raised the outbreak status to the "highest level" of risk as health professionals had documented cases on every continent except Antarctica, with more than 90,000 cases worldwide and over 3,000 fatalities.

Uncertainty regarding the virus—including whether it will develop into a pandemic—continues to disrupt manufacturing and supply chains, roil financial markets, limit international travel, and exacerbate domestic political tensions in several countries around the world.

Since the WHO declaration on January 30, RiskIQ has observed a malicious spam campaign seeking to capitalize on this worldwide interest in the spread and impact of the virus.

Current Malware Phishing Operations

AZORult

As early as late January 2020, malware distributors launched a campaign with phishing emails that targeted companies whose supply chain operations and revenue streams the outbreak could disrupt. The targeted businesses came from a variety of sectors, including manufacturing, industrial, finance, transportation, pharmaceutical, and cosmetics.

The perpetrators have been sending emails with malicious Microsoft Word documents attached. The attachments install the AZORult malware, a credential and payment card information-stealer. Attackers have used AZORult via an exploit for CVE-2017-11882, which is a remote code execution flaw in Microsoft Equation Editor. When exploited successfully, the flaw allows attackers to execute remote code on a vulnerable machine once the malicious document is opened—even without user interaction.

(We have been unable to identify the cybercriminals behind the AZORult phishing campaign, but our initial suspicion is that they are based in Russia or Eastern Europe because this is where this particular malware is most commonly bought and sold.)

Emotet

Similarly, in Japan, phishing scams are spreading the Emotet Trojan by using malicious messages that purport to contain information about coronavirus. This scam capitalizes on a user's desire to learn more about the coronavirus threat. Included in the emails are Microsoft Office attachments that use malicious macros to infect recipients with Emotet.

Security researchers first identified the Emotet Trojan in 2014 when it was deployed against the financial sector. Emotet uses functionality that helps the software evade detection by some anti-malware products. It also has worm-like capabilities that help it spread to other connected computers. This functionality has led the Department of Homeland Security to conclude Emotet is one of the most costly and destructive pieces of malware, affecting government and private sectors as well as individuals and organizations.

In 2019, cybercriminals made Emotet even more dangerous by updating its attack methods with the ability to send victims emails from past messages, steal credentials from its victims to send outbound messages, and hijack victims' email accounts. These techniques make it easier for hackers to trick users into thinking they are responding to a legitimate email.

Social Engineering

Another campaign cybercriminals are having success with capitalizes on conspiracy theories claiming the existence of "unreleased cures" being kept from the public. While these attacks initially targeted people in the United States and Japan, there is some evidence the perpetrators are now targeting Australia and Italy. The email urges recipients to click on an embedded link to receive information about the "cure." The link then leads users to a fake DocuSign page where they're encouraged to share personal credentials to receive the information.

Beware of Fake Domains

Some phishing campaigns are incorporating fake domains designed to look like the U.S. Centers for Disease Control and Prevention (CDC) and the WHO. These fake domains, e.g., cdcgov.org or cdc.gov.org., are sent via phishing emails and appear to come from the CDC (CDC's legitimate site is cdc.gov.). The emails urge victims to click on a link to download a document on health and safety measures regarding the spreading of coronavirus. Victims believe the link is taking them to the CDC website, but it redirects them to a fake site that looks like a Microsoft Outlook login page. Here, victims are asked to enter their username and password.

Cybercriminals are using a similar method with fake WHO credentials. In these cases, if users click the link in the email, they are led to a webpage that looks similar to the WHO website. However, this fake site contains a popup screen asking them to verify the username and password associated with their email address. As with the phony CDC website scam, if someone enters their credentials, the information is sent to the attackers.

Same Old Health Scare Playbook

Many of the attack methods cybercriminals are using have been deployed during previous international health scares. The only significant difference is the improvements they have made to their attack tools.

- **Influenza Pandemic (2019):** Cybercriminals conducted a malspam campaign that pretended to be from the Centers for Disease Control and Prevention (CDC) about a new flu pandemic. The emails contained a malicious attachment that, when opened, installed the GandCrab v5.2 Ransomware on the target's computer (GandCrab fell out of favor in 2019, but was possibly replaced by Sodinokibi/REval ransomware.).
- **Zika Virus (2016):** Researchers discovered an email purporting to be from Saúde Curiosa, a health and wellness website in Brazil. Within the email were links and attachments claiming to be instructions on how to eliminate the virus and the mosquitoes that spread it—one of the links, which infected computers with a form of malware called JS.Downloader was clicked more than 1,500 times. JS.Downloader remains in use by attackers.
- **Ebola Outbreak (2014):**
  - Cybercriminals sent emails with an attached report on Ebola. Users who clicked on the report activated Trojan.Zbot (a.k.a Zeus) malware.
  - Cybercriminals sent emails posing as a well-known telecom and ISP and offered a presentation on the Ebola virus. The email came with a zip file that installed Trojan.Blueso malware.
  - Cybercriminals sent an email which claimed a cure for Ebola had been discovered and that the news should be covering it. Users who clicked on the link in the email were infected with Backdoor.Breut malware.
  - While none of these older malware formats appear to be a significant threat to organizations today, cybercriminals continue to deploy similar or updated versions.
- **AIDS Virus (1989)**
  - The first known healthcare-focused ransomware attack targeted AIDS researchers in 1989 and was called the "AIDS virus." This virus came on a floppy disk and scrambled the contents of its victims' computers by encrypting filenames and offering to unlock them in return for a "licensing fee" would be transferred to an offshore bank account. Today, modern ransomware is produced by hackers who have benefited from decades of virus development and who take advantage of industry-standard cryptography to attack their targets.

Expect Ransomware Attacks Next

In the past, AZORult has been used to download ransomware as a secondary infection. In 2018, cybercriminals used AZORult in a massive email campaign to distribute Hermes ransomware. In this case, the victims first lost their credentials, cryptocurrency wallets, and more before losing access to their files in the subsequent ransomware attack. That same year researchers discovered a new AZORult variant targeting computers around the world. Those infected had the Aurora ransomware installed as well as the information-stealing Trojan. Likewise, in 2019, the STOP ransomware family was deployed in conjunction with AZORult.

The Emotet Trojan has also been used in conjunction with ransomware. In 2019, Emotet was found to have partnered with TrickBot and Ryuk ransomware. This malware combo adapts Emotet to drop TrickBot and modifies TrickBot not only to steal data but also to download the Ryuk ransomware, which encrypts the machine. In this campaign, the attacker can take personal information, passwords, mail files, browser data, registry keys, and more, before encrypting the victim's machine and ransoming their data.

Consequently, RiskIQ assesses with a moderate-high level of confidence cybercriminals will follow a pattern we've seen before. We expect they will conduct layered attack campaigns similar to those of the recent past. And with a large pool of institutions, organizations, and individuals to target, they can be confident of success. Company executives, mid-level managers, administrators of local governments, and, of course, healthcare professionals all have a professional interest in following the latest developments around the spread of coronavirus. And it only takes one tired or overworked individual to click on what he or she believes is a legitimate alert or update.

Mitigating Your Risk

- For information about the coronavirus, visit the WHO's website.
- Only use trusted news sources for additional information.
- Do not click on links or open attachments in unsolicited email messages.
- Run up-to-date security software on your computer.
- Educate users to be on guard for threats, like Emotet, that present emails that appear to be unexpected replies to older email threads, emails that seem out of context, or messages from familiar names but are sent from unfamiliar email addresses.
- Ensure systems are patched on time.
- Update endpoint detection and response and anti-virus solutions deployed.
- Segregate networks to limit the reach of self-propagating malware.
- Review privileged access and users to enforce principles of least privilege.
- Keep up to date on blacklists of malicious IPs and compromised websites.

- Use an email security tool that features attachment inspection and disable the ability to run macros from attachments.
- Regularly back up your data on your system and store it offline or on a different network.
- Encrypt your sensitive data.
- Have an incident response plan ready.

RiskIQ's Solutions for Ransomware, Cyber Threats

RiskIQ's Executive Guardian®: RiskIQ uses internet-scale visibility to provide insight into emerging cyber threats. RiskIQ's team of cybersecurity experts and former intelligence officers minimize the likelihood of private data falling into the wrong hands and maintain visibility into security risks resulting from data exposure to protect executives, key employees, and brand reputation.

RiskIQ Digital Footprint®: Digital Footprint catalogs assets belonging to an organization by comprehensively searching the open web. RiskIQ's unique access to internet data at scale, including with ten years of internet data history, allows it to create a comprehensive picture of what assets are exposed to the open web. By identifying an organization's publicly-facing open ports, Digital Footprint helps organizations defeat ransomware attempts.

RiskIQ's PassiveTotal®: PassiveTotal empowers an organization's security analysts to identify potentially malicious infrastructure used by threat actors. PassiveTotal's proprietary, open-source, and third-party data sets combine to create a powerful tool for tracking potentially harmful infrastructure. PassiveTotal helps organizations understand threat infrastructure and identify indicators of compromise through crowd-sourced research into threat actors and malicious campaigns.

Click here to explore RiskIQ's suite of products designed to help you mitigate these and other cyber threats.

RISKIQ®

RiskIQ, Inc.
22 Battery Street, 10th Floor
San Francisco, CA. 94111

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com