SPECIAL REPORT

RANSOMWARE TAKES ADVANTAGE OF THE COVID-19 CHAOS

The chaos around the coronavirus, subsequent lockdown and economic turmoil has made a situation ripe for cyberattacks against individuals as well as companies and government entities. The latter categories offer bigger targets with the potential for bigger pay-outs.

Cybercriminals are taking advantage of the mayhem in many ways, but one type of attack stands out among the rest: ransomware.

Why is ransomware on the rise?

As the pandemic spread across the globe, people everywhere sought information that would ease their sense of uncertainty, or even give them some hope of returning to normal life. Google searches related to the coronavirus peaked in the US on March 15, 2020, according to Google Trends public data. Attempts for malicious attacks surged accordingly, although not entirely in parallel (see chart below), with 77 reported campaigns related to the pandemic observed by Skybox Research Lab between February 28 and May 31, 2020.

More than 60 percent of these reports were in April, when governments ordered lockdowns in dozens of countries. This situation created fertile ground for ransomware attacks. Often camouflaging the ransomware under the guise of new information about the coronavirus, attackers tried to lure their victims into clicking a malicious link. In Italy, one of the most badly hit countries in terms of COVID-19 infections,

PROTECT YOURSELF AGAINST THE THREAT OF RANSOMWARE

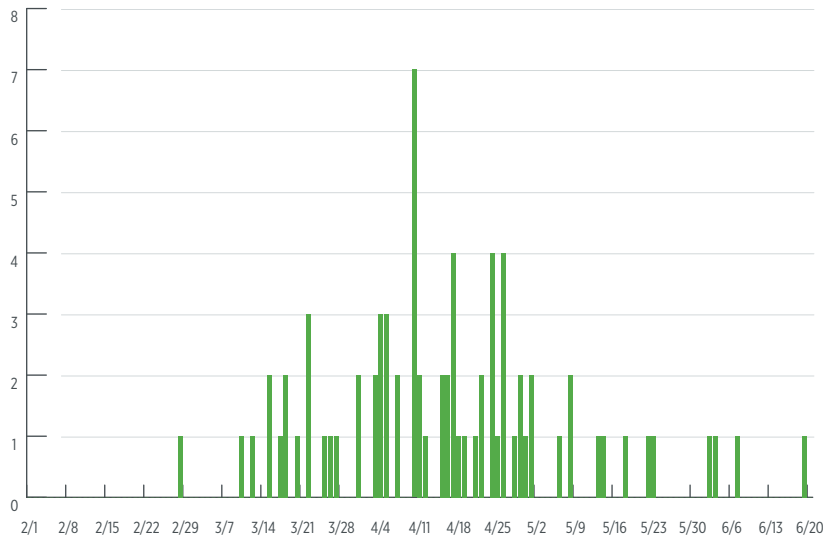
Good defense is the best offense. Proactive measures to reduce the risk of a successful ransomware attack are the best way to ensure your business can keep running smoothly.

- ✓ Educate employees on avoiding suspicious emails and links
- ✓ Ensure operating systems, software and applications are patched and up to date
- ✓ Regularly run anti-virus and anti-malware scans
- ✓ Mitigate potential damage by maintaining offline backups
- ✓ Create a continuity plan if an attack does occur

attackers created a web page mimicking the Italian Federation of Pharmacists website to lure users into downloading ransomware disguised as a COVID–19 dashboard. Other ransomware targeted users of different popular applications such as Android OS and Microsoft Office.

Daily Reports of COVID-19 Malware Campaigns

(February 1-June 20, 2020)



Who is vulnerable?

In addition to ordinary citizens seeking information on coronavirus, ransomware attacks during the pandemic also hit aid organizations, medical billing companies, manufacturers, transport agencies, government institutions and educational software providers. One category that stood out was health care systems.

Hospitals have been a preferred target for ransomware attacks for years, as locking access to patients' information such as drug history or surgery directives can result in delaying or even halting critical medical treatment. That's why hospitals are more prone to pay ransom than other attack victims. The COVID–19 pandemic, which stretched health care systems to their limits, eliminated any "breathing room" these systems may have had if attacked in normal times. That turned them into even easier prey to threat actors.

For example, on March 12 and 13, Brno University Hospital in the Czech Republic was hit by a major ransomware attack that caused a shutdown of its computer systems. The attack was reported a month later, along with another attack on a Czech public hospital. The publication drew an unequivocal response from the U.S. state department, which declared that anyone engaged in such malicious activity should "expect consequences." Although some ransomware operators have stated that they will no longer target health and medical organizations during the pandemic, it is a fact that others do not hesitate to cash in on the crisis.

What should my organization do if hit by ransomware?

If your network is affected by a ransomware, detecting and mitigating it should be based on a holistic approach. In a recent blog post, Microsoft Threat Protection Intelligence Team pointed out that using indicators of compromise (IOCs) alone to determine impact from such an attack is not enough, as it is a common practice for ransomware threat actors to change their tools and systems once they determine the detection capabilities of their victims.

A best practice is to investigate and identify all endpoints affected. Assume that all the credentials present on those endpoints are now available to the attackers, whether the accounts associated with them were logged on when the attack started or not.

The FBI guidelines for ransomware attack response emphasize isolating the affected devices as soon as possible. This could be done by removing these systems from the network, or even by shutting them down in order to prevent the ransomware from attacking the network and shared drives. It's also recommended to isolate or power off affected devices that have not been fully corrupted yet, in order to gain more time to clean and recover data. Backup data and devices should be taken offline immediately. If some of the hijacked data is still available – make sure to secure it. After taking these steps, change all online account passwords and network passwords. You should also change all system passwords once the ransomware is removed from the system.

When should you pay attackers, if at all?

Paying the ransom demanded by the attackers to end the attack is highly inadvisable under any circumstances. Doing so, the FBI explains, could have dire consequences one might not consider when making decisions under the pressure of an attack. First, paying the attackers does not guarantee regaining access to the compromised devices. Some attackers have never provided their victims with decryption keys to the compromised data even if their demands were satisfied. That was the case with WannaCry, maybe the most widespread ransomware attack to date.

Second, even if paying ransom has ended the attack, victims who paid ransom have been targeted again by threat actors, probably because of their cooperation. Moreover, some attackers see the victim's willingness to pay ransom as a reason to push their victims to pay more money than originally demanded. Finally, paying a ransom to attackers may encourage this criminal business model, perpetuating its existence. As we've seen during a crisis, ransomware can not only cause financial damage but also risk lives.

While many ransomware attacks are initiated via phishing or other social engineering techniques, some of the most notable ransomware attacks — like WannaCry — have exploited known vulnerabilities.

See how Skybox intelligently prioritizes exploitable and exposed vulnerabilities for immediate remediation

Get the solution brief >

How do I prevent my organization from being hit by ransomware?

The best way to avoid being exposed to ransomware, or any type of malware, is to be a cautious and conscientious computer user. That is particularly important given the COVID–19 crisis, as US-CERT points out that widespread fear–inducing events like disease outbreaks are often used as the pretext for social engineering lures. It means, for instance, going directly to the sites of health services rather than following links claiming to be from them. It should be noted that, as threat actors are becoming more sophisticated and savvy, even legitimate sources of information may be used to spread malware.

Standard measures such as keeping your operating systems, software and applications current and up to date are also important, as well as ensuring anti–virus and anti–malware tools are set to automatically update and run regular scans.

Backup may not prevent being hit by a ransomware but can dramatically mitigate its impact. Make sure to update your data regularly and often, and double-check that those backups were completed. It's essential that backups are secure and not connected to the network and computers they're backing up.

Finally, creating a continuity plan for your organization in case it falls victim to a ransomware attack could also help mitigate its impact, especially during a crisis such as the world is experiencing now.

SKYBOX SECURITY

www.skyboxsecurity.com

Copyright © 2020 Skybox Security, Inc. All rights reserved. Skybox is a trademark of Skybox Security, Inc. All other registered or unregistered trademarks are the sole property of their respective owners. 06252020

ABOUT SKYBOX SECURITY

Skybox provides the industry's broadest cybersecurity management platform At Skybox Security, we provide you with cybersecurity management solutions to help your organization innovate rapidly and with confidence. We get to the root of cybersecurity issues, giving you better visibility, context and automation across a variety of use cases. By integrating data, delivering new insights and unifying processes, you're able to control security without restricting operational agility. Skybox's comprehensive solution unites different security perspectives into the big picture, minimizes risk and empowers security programs to move to the next level. With obstacles and complexities removed, you can stay informed, work smarter and drive your organization forward, faster.