Hacking group is targeting US hospitals with Ryuk ransomware

bleepingcomputer.com/news/security/hacking-group-is-targeting-us-hospitals-with-ryuk-ransomware/

Lawrence Abrams

By
Lawrence Abrams

- October 29, 2020
- 07:31 AM
- 0

In a joint statement, the U.S. government is warning the healthcare industry that a hacking group is actively targeting hospitals and healthcare providers in Ryuk ransomware attacks.

Today, the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS) announced a call with the healthcare industry to warn them of an 'Increased and Imminent Cybercrime Threat.'

Email to healthcare providers

On this call, the U.S. government warned healthcare providers that Ryuk ransomware is actively targeting the healthcare industry and that proper steps should be taken to secure their systems.

These steps include preparing network lockdown protocols, review incident response plans, install patches on Windows servers and edge gateway devices, limit personal email, and create strategies on where to redirect patients in the event of an attack.

One source told BleepingComputer that it was recommended that all devices should be turned off when not in use in case of an attack.

Since the call, CISA, FBI, and HHS have released a joint advisory containing information about the Ryuk ransomware threat, including indicators of compromise (IOC).

"CISA, FBI, and HHS have credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers. CISA, FBI, and HHS are sharing this information to provide warning to healthcare providers to ensure that they take timely and reasonable precautions to protect their networks from these threats," the advisory states.

In the past two days, Sky Lakes Medical Center in Oregon and St. Lawrence Health System in New York were both hit in Ryuk ransomware attacks that impact the treatment of patients. Last month, hospital operator Universal Health Services was hit by a corporate-wide Ryuk attack, which impacted over 200 medical facilities nationwide.

UNC1878 hacking group behind threat

Charles Carmakal, senior vice president and CTO of Mandiant, told BleepingComputer that a hacking group known as UNC1878 is behind the Ryuk attacks on the healthcare industry.

"We are experiencing the most significant cyber security threat we've ever seen in the United States. UNC1878, an Eastern European financially motivated threat actor, is deliberately targeting and disrupting U.S. hospitals, forcing them to divert patients to other healthcare providers. Patients may experience prolonged wait time to receive critical care," Carmakal said in a statement to BleepingComputer.

In a conversation with Carmakal, BleepingComputer was told that this group is highly efficient, with ransomware being deployed in some cases within 45 minutes of a network being compromised.

Victims are then left with 7-8 figure ransom demands to get a decryptor for their encrypted files.

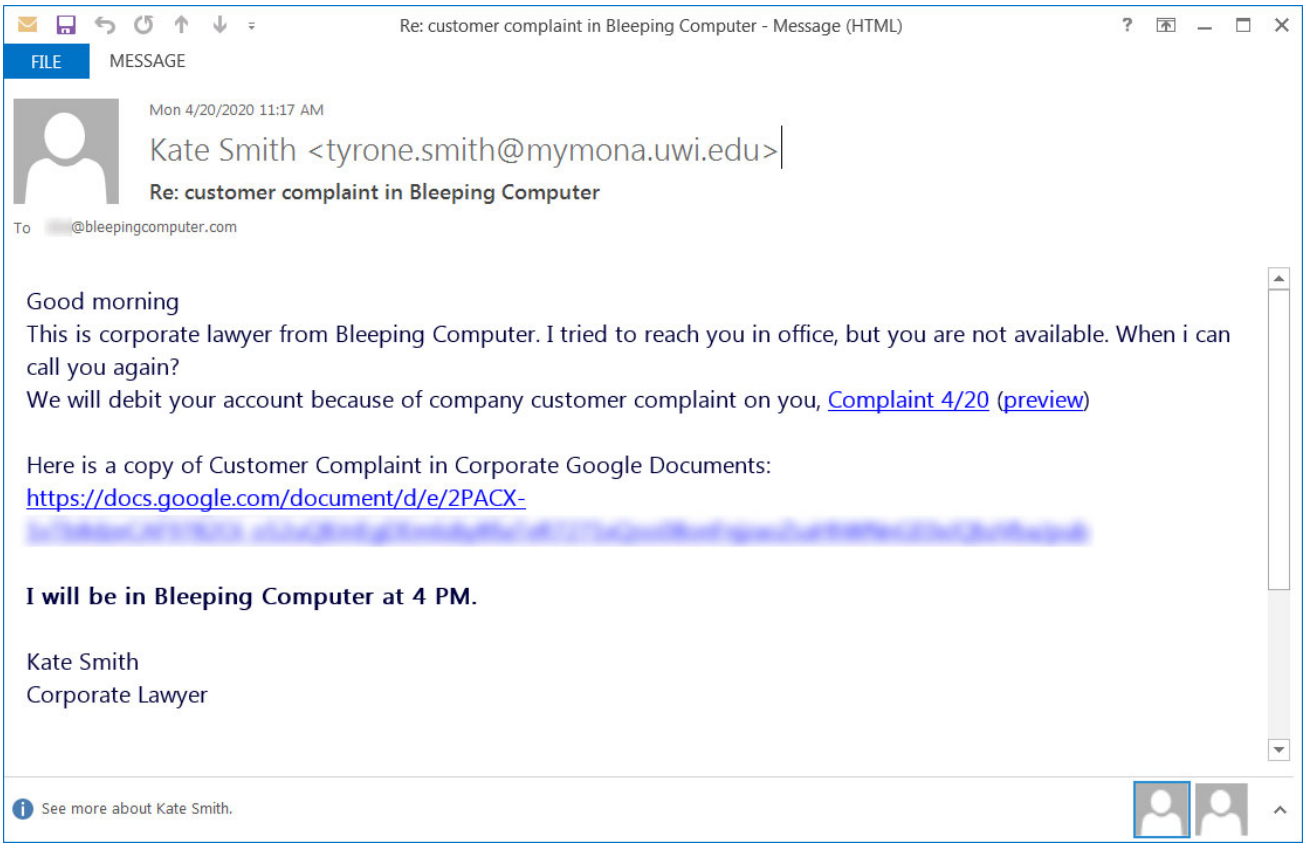
At the beginning of the Coronavirus pandemic, BleepingComputer reached out to different ransomware operations to see if they would continue to attack healthcare and medical organizations.

While most ransomware gangs said they would decrypt hospitals for free, Ryuk ransomware did not respond to our queries.

From BazarLoader to Ryuk

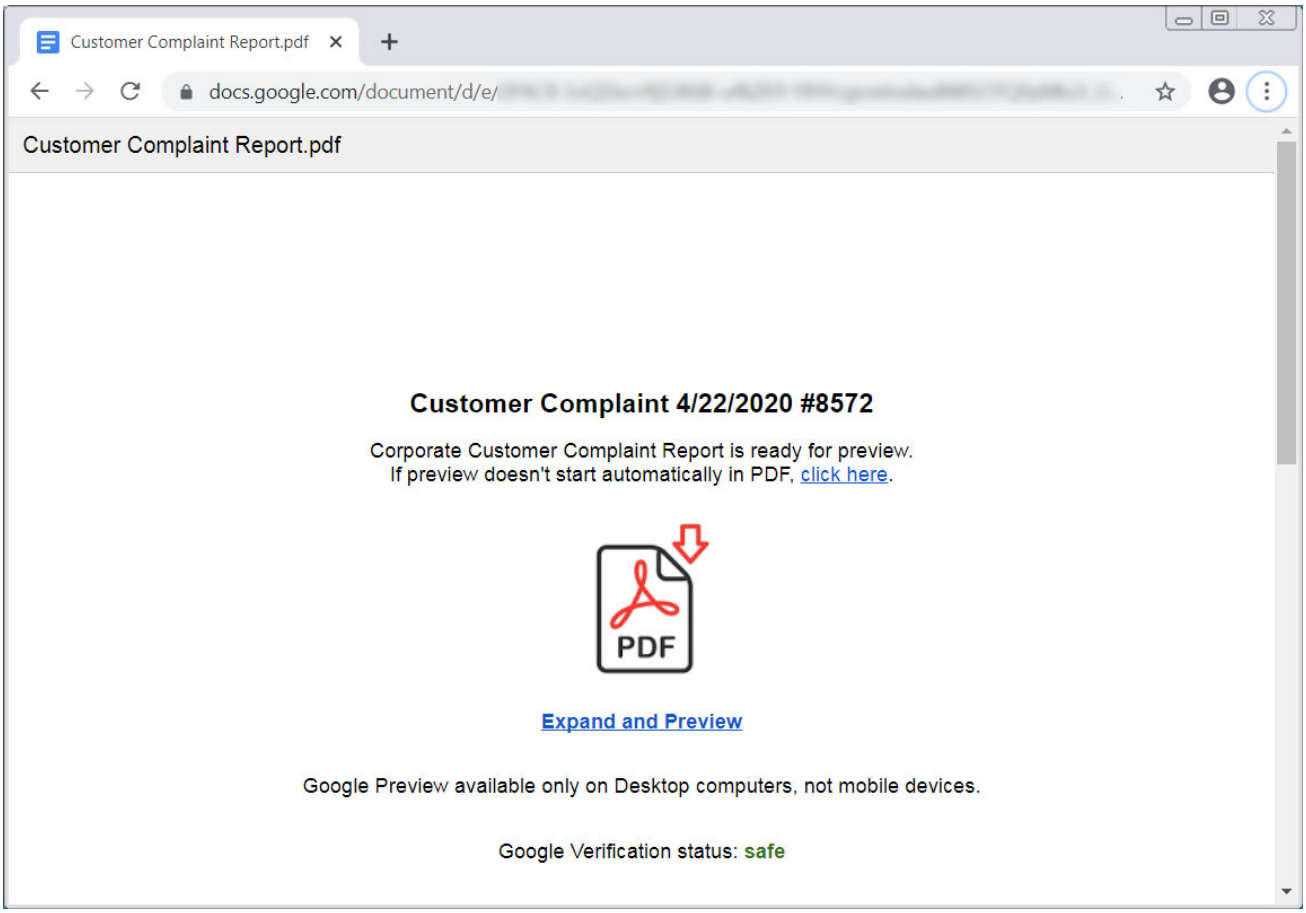
Lately, Ryuk attacks usually start with a phishing campaign that installs the BazarLoader/KegTap infection on a recipient's computer.

The phishing emails are targeted at a particular organization and can include lures ranging from invoices to customer complaints, as shown below.



BazarLoader phishing email directed at BleepingComputer

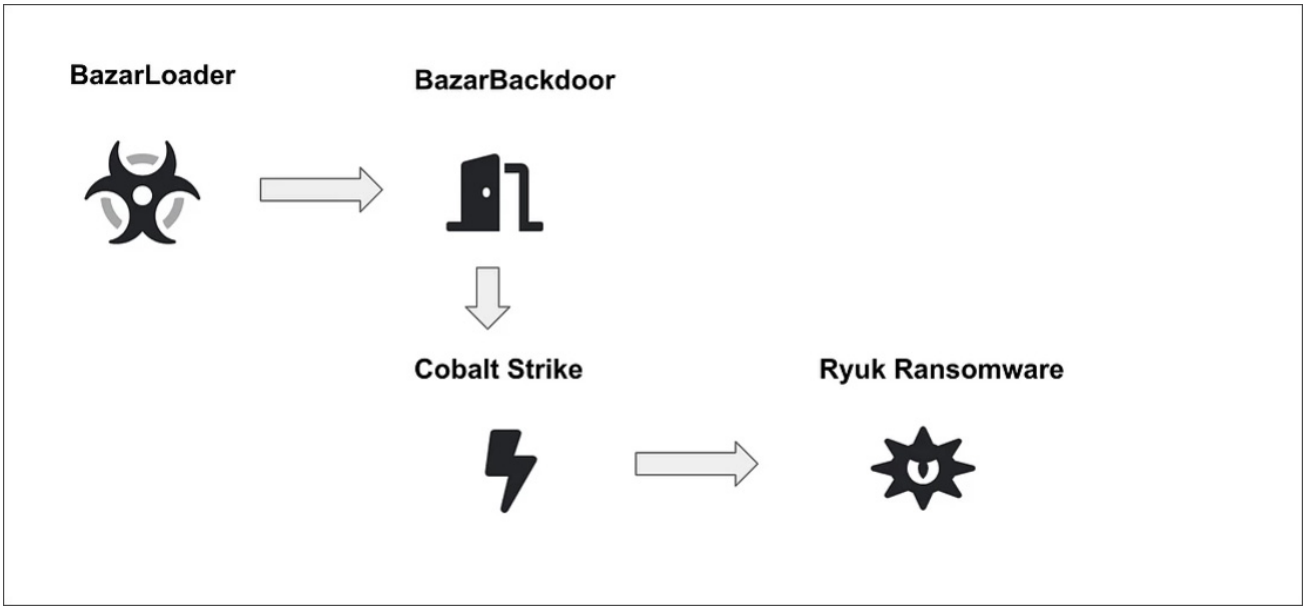
These emails include links to Google Docs that pretend to be PDFs that cannot be previewed correctly. These docs prompt the user to click on a link to download the document.



Phishing email landing page

The downloaded file is an executable that will install the BazarLoader infection onto a victim's computer when executed.

When installed, BazarLoader will eventually deploy Cobalt Strike, which allows threat actors to remotely access the victim's computer and use it to compromise the rest of the network.



BazarLoader attack flow

Source: Advanced Intel

To quickly gain Windows domain admin credentials, Carmakal told BleepingComputer that the group had been seen using the Windows ZeroLogon vulnerability. For this reason, users must install necessary patches on all Windows servers.

After gaining access to a Windows domain controller, the attackers deploy the Ryuk ransomware on the network to encrypt all of its devices, as illustrated in the diagram above.

Advanced Intel's Vitali Kremez told BleepingComputer that their Andariel threat prevention platform has been tracking an increased amount of attacks against healthcare using BazarLoader.

"The crime group behind continues to target various industries including healthcare. Currently, the healthcare and social services targeting comprises 13.36% of the total victim by industries," Kremez told BleepingComputer.

FireEye has also released a report today with TTPs that can be used to learn more about UNC1878 attack methods.

Carmakal told BleepingComputer that these attack methods are constantly changing, so the listed IOCs and TTPs would likely change in new attacks.

Related Articles:

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

US Senate: Govt’s ransomware fight hindered by limited reporting

- Healthcare
- Hospital
- Ransomware
- Ryuk
- UNC1878

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: