Ryuk Ransomware Attacked Epiq Global Via TrickBot Infection

bleepingcomputer.com/news/security/ryuk-ransomware-attacked-epiq-global-via-trickbot-infection/

Lawrence Abrams

By
Lawrence Abrams

- March 4, 2020
- 05:28 PM
- 0

Legal services and e-discovery giant Epiq Global took their systems offline on Saturday after the Ryuk Ransomware was deployed and began encrypting devices on their network.

On March 2nd, legal reporter Bob Ambrogi broke the news that Epiq had globally taken their systems offline after detecting a cyberattack.

This outage affected their e-Discovery platforms, which made it impossible for legal clients to access documents needed for court cases and client deadlines.

Epiq later stated that they were affected by a ransomware attack and took their systems offline to contain the threat.

"On February 29, we detected unauthorized activity on our systems, which has been confirmed as a ransomware attack. As part of our comprehensive response plan, we immediately took our systems offline globally to contain the threat and began working with a third-party forensic firm to conduct an independent investigation.

Our technical team is working closely with world class third-party experts to address this matter, and bring our systems back online in a secure manner, as quickly as possible.

Federal law enforcement authorities have also been informed and are involved in the investigation.

As always, protecting client and employee information is a critical priority for the company. At this time there is no evidence of any unauthorized transfer or misuse or exfiltration of any data in our possession."
Later that night, TechCrunch reported that they were told that the attack affected all of Epiq's 80 global offices and their computers.

Epiq Global's attack started with a TrickBot infection

Today a source in the cybersecurity industry exclusively shared information with BleepingComputer that sheds light on how Epiq Global became infected.

In December 2019, a computer on Epiq's network became infected with the TrickBot malware.

TrickBot is most commonly installed by the Emotet Trojan, which is spread through phishing emails.

Once TrickBot is installed, it will harvest various data, including passwords, files, and cookies, from a compromised computer and will then try spread laterally throughout a network to gather more data.

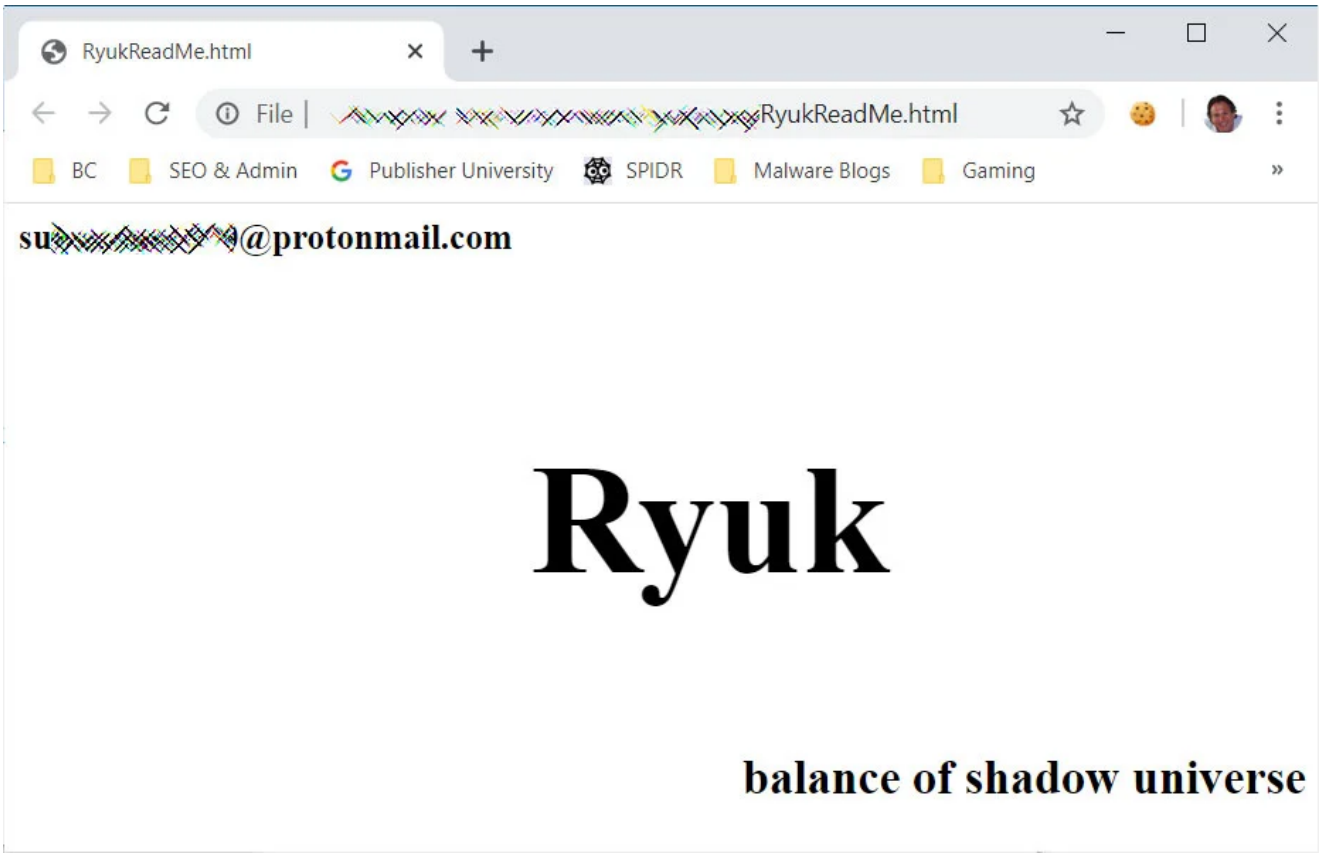
When done harvesting data on a network, TrickBot will open a reverse shell to the Ryuk operators.

The Ryuk Actors will then have access to the infected computer and begin to perform reconnaissance of the network. After gaining administrator credentials, they will deploy the ransomware on the network's devices using PowerShell Empire or PSExec.

In Epiq Global's case, Ryuk was deployed on their network on Saturday morning, February 29th, 2020, when the ransomware began encrypting files on infected computers.

Ransom Note Created

When encrypting files, the ransomware will create a ransom note named RyukReadMe.html in every folder. All files that were encrypted would also have the **.RYK** extension appended to them.



Epiq Global's Ryuk Ransom Note

While Ryuk is considered a secure ransomware without any weaknesses in its encryption, Emsisoft's Brett Callow has told BleepingComputer that there may be a slight chance they can help recover files encrypted by the Ryuk ransomware.

“Companies affected by Ryuk should contact us. There is a small - very small - chance that we may be able to help them recover their data without needing to pay the ransom,” Callow told BleepingComputer.com.

While the chances are very small, if your devices are encrypted by the Ryuk Ransomware it does not hurt to check with Emsisoft.

BleepingComputer has reached out to Epiq with further questions about this attack, but have not heard back at this time.

Related Articles:

New Bumblebee malware replaces Conti's BazarLoader in cyberattacks

TrickBot cybercrime group linked to new Diavol ransomware

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

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.