VOTIRO

THALES

Ryuk: Everything You Need to Know About the Ransomware Targeting U.S. Governments & Government Agencies

Contents

Ryuk: Everything You Need to Know About the Ransomware Targeting U.S. Governments & Government Agencies

Cyber extortion has become an attack of choice for hackers. It is estimated that attacks cost the US more than $7.5 billion in 2019 and malware attacks can be expected to increase in 2020. As of now, U.S. law generally does not prohibit paying a ransom, but this may change in the future.

First discovered in mid-August 2018, Ryuk is a type of ransomware that penetrates a target and uses encryption to block access to files, systems, or networks until a ransom is paid. These ransomware attacks cause significant damage, including data loss, disruption of service, downtime, damage to the enterprise or organization's reputation, and loss of revenue. Currently, Ryuk ransomware is one of the most prevalent variants in the state, local, tribal, and territorial (SLTT) government threat landscape, with infections steadily increasing. Ryuk also targets federal government agencies and military operations.

Where Did Ryuk Ransomware Come From?

The fact that Ryuk is a fictional character from the Japanese comic series Death Note, does not reveal much about the malware under the same name. Instead, criminal groups are often tied to their malware by searching for similarities in the code base, structure, language, and attack vectors. Back in 2018, Check Point found a link between Ryuk and another type of ransomware called Hermes. Comparisons between the two indicate that Ryuk was derived from the Hermes source code, although Ryuk only targets enterprise environments and includes modifications such as removing anti-analysis checks.

This connection may also link Ryuk with the North Korean Advanced Persistent Threat (APT) Lazarus Group, a cybercrime group that has been closely connected with Hermes ransomware in the past.

Others, including cybersecurity experts at CrowdStrike, McAfee, FireEye and Kryptos Logic believe that the cybercriminals behind Ryuk ransomware may be linked to two Russian-based cyber-criminal entities: Wizard Spider, the operator of TrickBot and CryptoTech, an organization also linked to Hermes.

As Ryuk's ransom payments vary widely in amounts and methods, some experts feel there may be more than one criminal group operating Ryuk ransomware. In addition, Ryuk may be sold on the black market to other cyber-criminals seeking to build their own versions of the ransomware.

How Does Ryuk Ransomware Operate?

The cybercriminals behind Ryuk ransomware employ a multi-stage scheme to ensure this malware penetrates their target. Typically, the campaign starts with phishing emails, or by clicking on a deceptive link, or via Remote Desktop Services. When an unsuspecting user unsuspectingly executes the embedded malicious macro, an Emotet bot (Detection name: Trojan-Banker. Win32.Emotet) will automatically be downloaded and infect the machine.

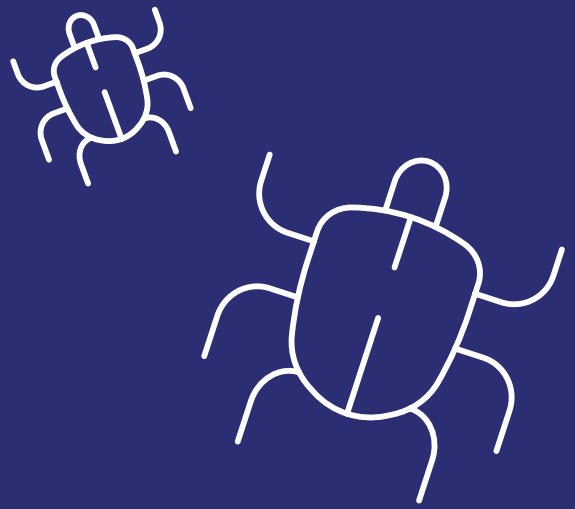
Once the Emotet bot penetrates the machine, it downloads and installs the second piece of malware – Trickbot (verdict: Trojan. Win32.Trickster) – into the infected system. This Trickbot enables cybercriminals to have full visibility into the network and to perform extensive mapping and identification of assets. These criminals can now determine whether the target is worthwhile – for example, a large municipal network or a high-profile enterprise – and if so, they will deploy the Ryuk ransomware to infect as many endpoints and servers as possible, by encrypting both the local drives and network shared folders – and their backups – of the compromised network.

Encrypted files will receive an additional extension (.RYK), and a ransom note "RyukReadMe.txt" from the criminals will appear in every folder on the system. Ryuk generally demands payment via Bitcoin cryptocurrency, and the ransom is typically between 15-50 Bitcoins, which is about $100,000-$500,000, an amount that is ten times the average asking amount, according to ransomware specialists Coveware.

Ryuk's ability to target backups and use anti-recovery tools are more sophisticated than other types of ransomware, which is why targets generally fail in their recovery efforts unless backups have been stored offline.

How Prevalent is Ryuk Malware?

As a ransomware targeting enterprises and governments, Ryuk has been wreaking havoc all over the world, although some countries have been affected more than others. According to Kaspersky Security Network's known cases, the top three countries affected are Germany, China, and Algeria, with the United States ranking at 7th in the world for Ryuk attacks. This type of attack is on the rise in the United States. See chart below for the percentage of users attacked in each country by Ryuk, relative to users attacked worldwide by this malware:



Country	Percent
Germany	8.60%
China	7.99%
Algeria	6.76%
India	5.84%
Russian Federation	5.22%
Iran	5.07%
United States	4.15%
Kazakhstan	3.38%
United Arab Emirates	3.23%

Ryuk Ransomware Attacks in the US

As of March 2020, there have been 32 publicized Ryuk ransomware attacks in the US on government entities. There have also been attacks on government contractors, retailers, healthcare providers and hospitals, manufacturers, and professional services firms.

Notable Ryuk Ransomware Attacks on U.S. Governments

Durham, North Carolina: In March 2020, the city of Durham became the latest target of Ryuk ransomware, when the attack — which arrived when a city employee opened a phishing email — took down 80 servers. The attack affected widespread municipal and county government services, taking down systems from the police to fire services.

Department of Defense Contractor, Electronic Warfare Associates (EWA): In January 2020, Ryuk Stealer ransomware attacked the systems of U.S. government contractor, EWA. EWA clients include the Department of Homeland Security, Department of Defense, and Department of Justice. Experts suspect a phishing email to be the attack vector and data exfiltration to be the goal of the attack.

City of New Orleans: In December 2019, New Orleans became victim to a Ryuk ransomware attack via a phishing email. The malware attack impacted over 450 servers and 3500 laptops and caused the city to declare a state of emergency. Ultimately, the attack cost the city $3 million in mitigation and recovery costs, a sum that was covered by the city's cyber insurance policy.

New Bedford, Massachusetts: In July 2019, a Ryuk ransomware attack infected a network of 200 systems and over 3,800 laptops and workstations in the city of New Bedford, Massachusetts. The hackers reportedly demanded a $5.3 million ransom. However, New Bedford attempted to negotiate the sum and offered $400,000 in bitcoins to contain the malware and decrypt the files. The counter-offer was refused, and the city's IT staff instead chose to restore the systems from backups. The ultimate cost of recovery and mitigation is unknown.

Lake City, Florida: In June 2019, a Ryuk ransomware attack disrupted the entire computer network of Lake City, FL. Police had to issue paper tickets, the 911 line was not fully operational, and the city's water supply grid went offline. After failing to resolve the issue on their own using an outside security consultant, the city paid the Bitcoin equivalent of $460,000 to recover its data, of which all but $10,000 was covered by insurance. This attack came only two weeks after another small Florida city, Riviera Beach, paid the Bitcoin equivalent of $600,00 in ransom to bring their systems back online.

Tips to Prevent Ryuk from Affecting Your Networks

CISOs and IT administrators should be proactive in protecting their enterprises against Ryuk ransomware attacks. Some suggested actions:

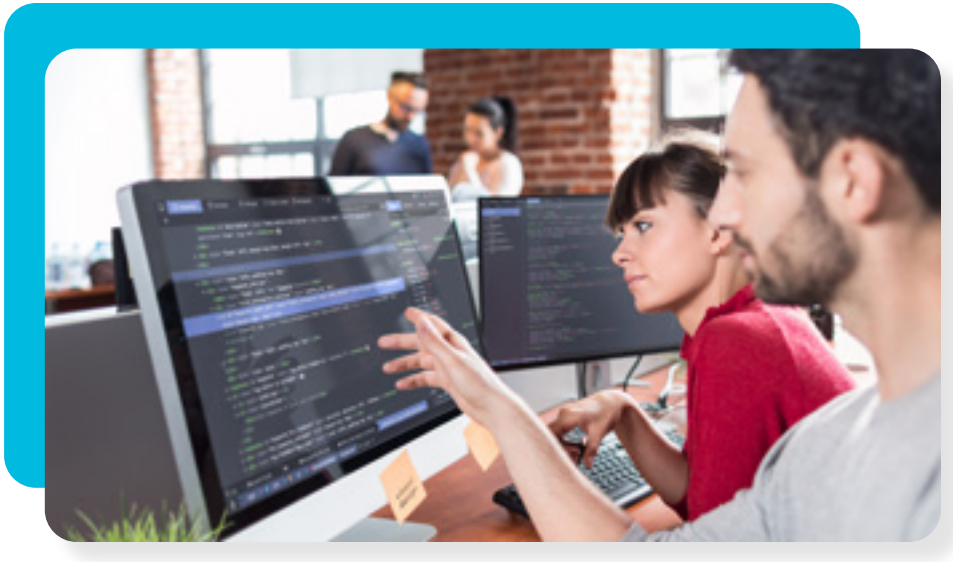
Deploy a solution that sanitizes all incoming files from threats: Positive Selection technology (an evolution of Content, Disarm & Reconstruction technology) is proven to be highly effective in neutralizing external malicious threats while preserving the integrity and functionality of the original file. This technology applies to all files and email files incoming into an organization, whether as attachments, downloads from the web, or files uploaded into the corporate network.

Authenticate users: Utilize a password management system and single sign-on services for all users. Allow access to mapped drives to specific roles only. Determine which authentication process works best for the enterprise.

Minimize attack surface: Ensure that all software is up to date and adequately patched across all endpoints.

Automated scans: Implement a solution that proactively and continuously scans your network for malware and takes steps to fix it before any significant damage ensues.

Backup Your Data: Backup your critical data in the cloud. Consider using third-party storage systems to maintain critical stat outside the primary enterprise network.



Summary

Ryuk ransomware presents a serious threat to enterprises and government organizations everywhere. Consequences of a ransomware attack are significant. No enterprise or governmental organization is immune. CISOs and IT administrators can take some key steps to protect important systems and networks, such as putting protocols in place to limit damage, deploying technical solutions— such as Positive Selection technology – to filter email files, email attachments, and other incoming files, and ensuring all data is properly backed up. With Ryuk malware, the absolute best protection is prevention.

About Votiro Secure File Gateway

Votiro Secure File Gateway: 100% Protection From Weaponized Files

Votiro introduces the Votiro Secure File Gateway: the only solution that guarantees complete protection from weaponized files. Unlike detection-based file security solutions that scan for suspicious elements and block some malicious files, Votiro's revolutionary Positive Selection™ technology singles out only the safe elements of each file, ensuring every file that enters your organization is 100% safe.

When an email containing a malicious file enters an enterprise's communications network, Positive Selection technology rebuilds the file, transferring over only the vendor-approved, known good content. This leaves the malicious code behind while allowing the file to retain its full usability and functionality.

All the functionality that users need for working with a file, such as copying text, handling bookmarks, keeping content on the original pages, using active content and embedded objects, running macros, and searching, is preserved.

Founded in 2010 by leading file security experts, Votiro's new approach to file security works invisibly in the background, completely eliminating threats while ensuring zero interruption to business.

Completely Secure Files, No Matter the Source:

Secure File Gateway for Email: Completely secure every email that enters your organization.

Secure File Gateway for Downloads: Secure everything employees download, no matter what it is or where it came from.

Secure File Gateway for Web Uploads: Secure all file uploads and receive documents completely risk-free.

Experience 100% Secure For Yourself

See for yourself how easy it is to safeguard your organization with the Votiro Secure File Gateway. Votiro Secure File Gateway is available for sale to the U.S. Federal Government exclusively through Thales Trusted Cyber Technolgies.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled. For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com