May 8, 2020

NTIC CYBER CENTER ALERT

Snake Ransomware Targets Enterprise Networks

NTIC Cyber Center members,

This alert is being provided for informational purposes and for potential use to protect systems, networks, and data against this cyber threat at the sole discretion of recipients. As the cyber threat landscape is ever-evolving and attribution can be difficult, the NTIC Cyber Center makes no guarantees of the accuracy of this information during and after the dissemination of this alert as indicators of compromise (IoCs) and adversary tactics, techniques, and procedures (TTPs) may change. Recipients are urged to use caution before implementing any changes to systems, software, and procedures.

SUMMARY

First detected in January 2020, Snake is a ransomware variant that is currently targeting enterprise networks around the world. Snake can infect systems running Windows OS and appends a random five character string to the extensions of encrypted files. It also drops a ransom note named Fix-Your-Files.txt or Decrypt-Your-Files.txt on the infected system's desktop that provides victims with instructions on how to pay the ransom to obtain the decryption key. Snake's capabilities include deleting Shadow Volume Copies to prevent file restoration and terminating various processes associated with ICS/SCADA systems, virtual machines, remote management tools, and network management software.

On May 4, 2020, ransomware identification website ID Ransomware began detecting a significant spike in Snake ransomware sample submissions, suggesting the operators of this campaign have dramatically increased their targeting of various organizations throughout the world. Victims of this campaign include Germany-based healthcare organization Fresenius, Europe's largest private hospital operator, as well as an
unnamed French architectural firm and prepaid debit card company, according to cybersecurity website BleepingComputer. Although there is currently no publicly available information about Snake ransomware's network intrusion methods, large-scale targeted ransomware campaigns such as this have historically used stolen administrator account credentials, credential stuffing attacks, Remote Desktop Protocol (RDP) compromise, and Managed Service Provider (MSP) compromise to launch attacks against enterprise networks. Similar to Sodinokibi/REvil, Maze, Ryuk, BitPaymer, and DoppelPaymer ransomware campaigns, Snake ransomware threatens victims with the public release of their sensitive data if the ransom payment is not submitted within a specified period of time.

![Snake (Ekans) Submissions: Last 3 Months](Image)

*(ID Ransomware Sample Submission Tracker - Image Source: BleepingComputer.com)*

![Snake Ransom Note](Image)

*(Snake Ransom Note - Image Source: BleepingComputer.com)*
RECOMMENDATIONS

The NTIC Cyber Center recommends all network administrators maintain awareness of this and other ransomware threats and take proactive steps to reduce their organization's risk of becoming victimized in an attack. As ransomware operators increasingly steal and threaten to release victims' sensitive data publicly to pressure them into paying the ransom, we highly recommend encrypting data both at rest and in transit to help render the data useless if stolen. We also encourage conducting regular data backups and storing data securely off the network. Regular testing of these backups is critical to ensuring data can be successfully restored should the need arise. For a comprehensive list of prevention strategies, please download the NTIC Cyber Center's Ransomware Mitigation Guide.

The information contained in this alert is designated TLP:WHITE, subject to standard copyright rules, and may be distributed without restriction.

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

Disclaimer: This NTIC Cyber Center Cyber Alert is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up at one of our events, or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Visit www.ncrinel.org, click on Subscribe to Receive Our Products at the top of the page, and enter your information.