SamSam Ransomware | CISA

Published: 2018-12-03 · Archived: 2026-04-05 13:52:08 UTC

Summary

The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) and the Federal Bureau of Investigation (FBI) are issuing this activity alert to inform computer network defenders about SamSam ransomware, also known as MSIL/Samas.A. Specifically, this product shares analysis of vulnerabilities that cyber actors exploited to deploy this ransomware. In addition, this report provides recommendations for prevention and mitigation.

The SamSam actors targeted multiple industries, including some within critical infrastructure. Victims were located predominately in the United States, but also internationally. Network-wide infections against organizations are far more likely to garner large ransom payments than infections of individual systems. Organizations that provide essential functions have a critical need to resume operations quickly and are more likely to pay larger ransoms.

The actors exploit Windows servers to gain persistent access to a victim's network and infect all reachable hosts. According to reporting from victims in early 2016, cyber actors used the JexBoss Exploit Kit to access vulnerable JBoss applications. Since mid-2016, FBI analysis of victims' machines indicates that cyber actors use Remote Desktop Protocol (RDP) to gain persistent access to victims' networks. Typically, actors either use brute force attacks or stolen login credentials. Detecting RDP intrusions can be challenging because the malware enters through an approved access point.

After gaining access to a particular network, the SamSam actors escalate privileges for administrator rights, drop malware onto the server, and run an executable file, all without victims' action or authorization. While many ransomware campaigns rely on a victim completing an action, such as opening an email or visiting a compromised website, RDP allows cyber actors to infect victims with minimal detection.

Analysis of tools found on victims' networks indicated that successful cyber actors purchased several of the stolen RDP credentials from known darknet marketplaces. FBI analysis of victims' access logs revealed that the SamSam actors can infect a network within hours of purchasing the credentials. While remediating infected systems, several victims found suspicious activity on their networks unrelated to SamSam. This activity is a possible indicator that the victims' credentials were stolen, sold on the darknet, and used for other illegal activity.

SamSam actors leave ransom notes on encrypted computers. These instructions direct victims to establish contact through a Tor hidden service site. After paying the ransom in Bitcoin and establishing contact, victims usually receive links to download cryptographic keys and tools to decrypt their network.

Technical Details

NCCIC recommends organizations review the following SamSam Malware Analysis Reports. The reports represent four SamSam malware variants. This is not an exhaustive list.

- MAR-10219351.r1.v2 – SamSam1
- MAR-10166283.r1.v1 – SamSam2
- MAR-10158513.r1.v1 – SamSam3
- MAR-10164494.r1.v1 – SamSam4

For general information on ransomware, see the NCCIC Security Publication at Stop Ransomware.

Mitigations

DHS and FBI recommend that users and administrators consider using the following best practices to strengthen the security posture of their organization's systems. System owners and administrators should review any configuration changes before implementation to avoid unwanted impacts.

- Audit your network for systems that use RDP for remote communication. Disable the service if unneeded or install available patches. Users may need to work with their technology venders to confirm that patches will not affect system processes.
- Verify that all cloud-based virtual machine instances with public IPs have no open RDP ports, especially port 3389, unless there is a valid business reason to keep open RDP ports. Place any system with an open RDP port behind a firewall and require users to use a virtual private network (VPN) to access that system.
- Enable strong passwords and account lockout policies to defend against brute force attacks.
- Where possible, apply two-factor authentication.
- Regularly apply system and software updates.
- Maintain a good back-up strategy.
- Enable logging and ensure that logging mechanisms capture RDP logins. Keep logs for a minimum of 90 days and review them regularly to detect intrusion attempts.
- When creating cloud-based virtual machines, adhere to the cloud provider’s best practices for remote access.
- Ensure that third parties that require RDP access follow internal policies on remote access.
- Minimize network exposure for all control system devices. Where possible, disable RDP on critical devices.
- Regulate and limit external-to-internal RDP connections. When external access to internal resources is required, use secure methods such as VPNs. Of course, VPNs are only as secure as the connected devices.
- Restrict users' ability (permissions) to install and run unwanted software applications.
- Scan for and remove suspicious email attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.

Additional information on malware incident prevention and handling can be found in Special Publication 800-83, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, from the National Institute of Standards and Technology.[1]

Contact Information

To report an intrusion and request resources for incident response or technical assistance, contact NCCIC, FBI, or the FBI's Cyber Division via the following information:

- NCCIC
  - SayCISA@cisa.dhs.gov
  - 1-844-Say-CISA
- FBI's Cyber Division
  - CyWatch@fbi.gov
  - 855-292-3937
- FBI through a local field office

Feedback

DHS strives to make this report a valuable tool for our partners and welcomes feedback on how this publication could be improved. You can help by answering a few short questions about this report at the following URL: Website Feedback.

Revisions

December 3, 2018: Initial version
