# SamSam: Targeted Ransomware Attacks Continue

By About the Author

Archived: 2026-04-05 22:24:57 UTC

**UPDATE: November 29, 2018**
*Two Iranian nationals have been indicted in the U.S. for their alleged involvement in SamSam attacks. The FBI estimated that the SamSam group had received $6 million in ransom payments to date and caused over $30 million in losses to victims.*

The group behind the SamSam ransomware (Ransom.SamSam) has continued to mount attacks against entire organizations during 2018, with fresh attacks seen against 67 different targets, mostly located in the U.S.

SamSam specializes in targeted ransomware attacks, breaking into networks and encrypting multiple computers across an organization before issuing a high-value ransom demand. The group is believed to be behind the attack on the city of Atlanta in March, which saw numerous municipal computers encrypted. The clean-up costs for the attack are expected to run to over $10 million.

The group was also linked to the attack on the Colorado Department of Transportation, which resulted in clean-up costs of $1.5 million.

## Heavy concentration on the U.S.

During 2018, Symantec has to date found evidence of attacks against 67 different organizations. SamSam targeted organizations in a wide range of sectors, but healthcare was by far the most affected sector, accounting for 24 percent of attacks in 2018.

Why healthcare was a particular focus remains unknown. The attackers may believe that healthcare organizations are easier to infect. Or they may believe that these organizations are more likely to pay the ransom.

A number of local government organizations in the U.S. were also targeted by the group and at least one of these organizations is involved in administering elections. With the midterm elections in the U.S. taking place on November 6, the focus is naturally on cyber information operations and threats to voting data integrity. However, ransomware campaigns such as SamSam can also be significantly disruptive to government organizations and their operations.

The vast majority of SamSam's targets are located in the U.S. Of the 67 organizations targeted during 2018, 56 were located in the U.S. A small number of attacks were logged in Portugal, France, Australia, Ireland, and Israel.

While most ransomware families are spread indiscriminately, usually via spam emails or exploit kits, SamSam is used in a targeted fashion. The SamSam group's modus operandi is to gain access to an organization's network, spend time performing reconnaissance by mapping out the network, before encrypting as many computers as possible and presenting the organization with a single ransom demand.

The attackers have been known to offer to decrypt all computers for a set ransom and/or offer to decrypt individual machines for a lower fee. In many cases, ransom demands can run to tens of thousands of dollars to decrypt all affected computers in an organization. If successful, these attacks can have a devastating impact on victim organizations, seriously disrupting their operations, destroying business critical information, and leading to massive clean-up costs.

## How SamSam compromises organizations

The attackers behind SamSam go to great lengths to infect as many computers as possible in a targeted organization. Multiple software tools are used to carry out an attack and, in many cases, the entire process can take days to complete.

In order to carry out its attacks, the SamSam group makes extensive use of "living off the land" tactics: the use of operating system features or legitimate network administration tools to compromise victims' networks.

These tactics are frequently used by espionage groups in order to maintain a low profile on the target's network. By making their activity appear like legitimate processes, they hope to hide in plain sight.

For example, in one attack that took place in February 2018, more than 48 hours passed between the first evidence of intrusion and the eventual encryption of hundreds of computers in the targeted organization.

The first sign of an intrusion came when the attackers downloaded several hacking tools onto a computer in the targeted organization. Ten minutes later, the attackers began running scripts in order to identify and scan other computers on the organization's network. They used PsInfo, a Microsoft Sysinternals tool that allows the user to gather information about other computers on the network. This could allow them to identify the software installed on these computers. PsInfo may have been used to identify systems with business-critical files that could be encrypted for ransom. The attackers also used the freely available hacking tool Mimikatz (Hacktool.Mimikatz) against selected computers to steal passwords.

After this initial flurry of activity, the attackers returned two days later and, shortly after 5 a.m., loaded the SamSam ransomware onto the initial computer. Interestingly, two different versions of SamSam were loaded. It is likely that two versions were used in order to have an alternative at hand in case one version was detected by security software.

An hour later, the attacks began executing SamSam on multiple computers across the organization's network. This operation was carried out using PsExec, another Microsoft Sysinternals tool, which is used for executing processes on other systems. Five hours later, just under 250 computers on the network had been encrypted.

## Ongoing and potent threat

SamSam continues to pose a grave threat to organizations in the U.S. The group is skilled and resourceful, capable of using tactics and tools more commonly seen in espionage attacks.

A successful SamSam attack will likely be highly disruptive to any affected organizations. In the worst-case scenario, if no backups are available or if backups are encrypted by SamSam, valuable data could be permanently

lost in an attack. Even if an organization does have backups, restoring affected computers and cleaning up the network will cost time and money and may lead to reputational damage.

## Protection

The following protections are in place to protect customers against SamSam attacks:

- Ransom.SamSam
- Hacktool.Mimikatz

In addition, Symantec's Targeted Attack Analytics (TAA) is able to identify and flag "living off the land" activity associated with targeted attacks such as SamSam. To find out more about TAA, read our white paper *Targeted Attack Analytics: Using Cloud-based Artificial Intelligence for Enterprise-Focused Advanced Threat Protection*

## Best practices

Backing up important data is one of the key pillars of combating ransomware infections. However, as there have been cases of ransomware encrypting backups, it should not be a replacement for a robust security strategy.

Victims need to be aware that paying the ransom does not always work. Attackers may not send a decryption key, could poorly implement the decryption process and damage files, and may deliver a larger ransom demand after receiving the initial payment.

---