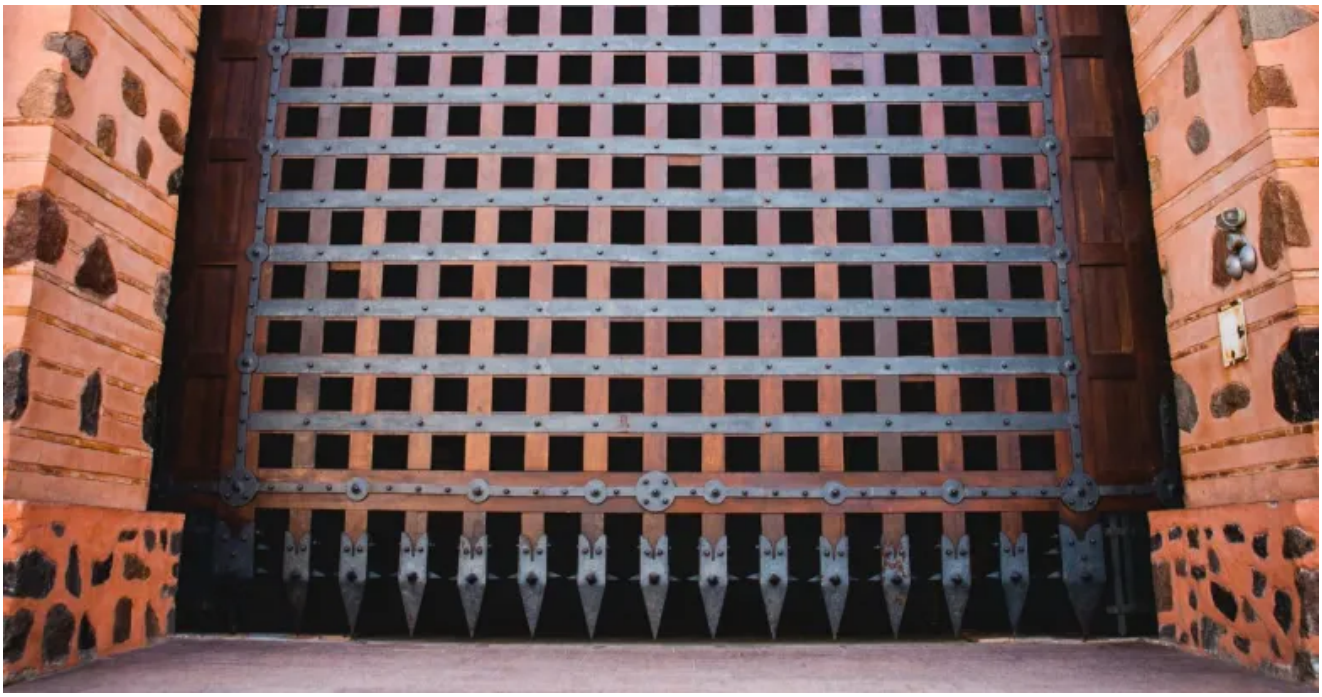
# How to defend yourself against SamSam ransomware

nakedsecurity.sophos.com/2018/08/02/how-to-defend-yourself-against-samsam-ransomware/

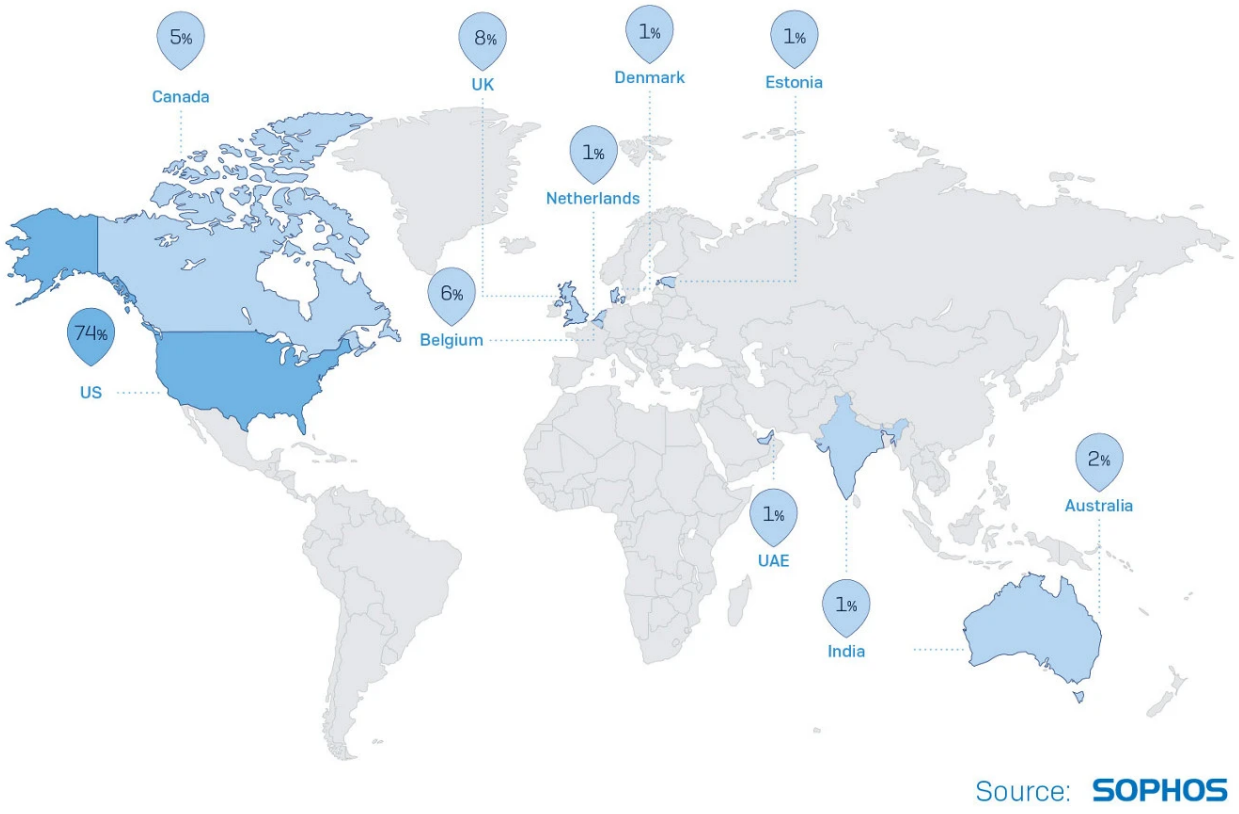
By Mark Stockley 02 Aug 2018



On Tuesday 31 July 2018 Sophos released the largest and most comprehensive research paper ever compiled on SamSam, a sophisticated and highly destructive piece of ransomware noted for its ability to put entire organisations under siege.

SamSam is different from most other ransomware – it's used sparingly, in a relatively small number of targeted attacks by a skilled team or individual. They break into and survey a victim's network before deploying and running the ransomware, just like a sysadmin deploying legitimate software.

## Percentage of SamSam victims by country, as identified by Sophos




Those unusual tactics create advantages for both attacker and defender.

The good news is that the SamSam attackers aren't looking for a challenge. They want easy targets, which means that getting a few of the basics right gives you a very good chance of keeping them out.

The bad news is that if they do get a foothold in your organisation they can dig in quickly. They don't deploy the SamSam malware until they're able to act as a Domain Admin, which gives them high ground from which to attack.

SamSam hackers have been seen changing their tactics during attacks and they will spend hours, and perhaps days, getting it right. If one approach doesn't work they'll try another and another, and if security software stops the malware from running, they'll look for ways to disable it.

As a result of Sophos's research into SamSam it has been able to further strengthen the protection provided by all of its products, and through membership of the Cyber Threat Alliance it's been able to benefit from other's insights and share the information it's learned with industry partners, strengthening everyone's protection.

Sophos believes that its products provide the best possible protection against SamSam. Like all good security software though, those products are most effective when they're deployed as part of a defence in depth strategy.

In this article we draw on the new research to look at some of the other important layers in that strategy, and how they can help you defend your organisation against SamSam.

## Be the smallest possible target

The best way to avoid trouble is to not be there when it starts.

So far, the SamSam attacker has entered victims' networks using exploits in internet-facing servers, most notably the JBoss application server, or by brute-forcing RDP (Remote Desktop Protocol) passwords.

### Patch

SamSam attacks have probably used the approaches mentioned above because they were the most successful or convenient at the time. There is no reason to suspect they won't switch to a different approach if a more effective alternative, such as a new exploit, emerges.

Because of that we recommend you don't focus on patching specific vulnerabilities but follow a strict patching protocol for operating systems and all the applications that run on them.

### Lock down RDP

Unless it's properly secured, RDP is a tempting target for all kinds of crooks, not just the SamSam attackers. We recommend you take the following steps to protect your organisation from attacks via RDP:

- Limit RDP access to people that need it.
- Don't allow Domain Admin accounts to use RDP.
- Require multi-factor authentication.
- Have a sensible policy for securing idle accounts.
- Limit the rate of password retries with the Security Policy Editor.
- Automatically lock accounts after a number of failed login attempts.
- Have staff access RDP through a VPN.
- Limit VPN access to specific IP addresses, ranges or geographies.
- Educate users about strong passwords and the dangers of password reuse.
- Encourage employees to use secure password managers.
- Test your staff's passwords to see how resilient they are.

### View your network like an adversary

Because there is no guarantee that the SamSam hackers won't change tactics it's important to understand what your network looks like to them. You can do that by undertaking regular vulnerability scans and penetration tests, and by performing periodic assessments, using third party tools like Censys or Shodan, to identify publicly-accessible ports and services across your public-facing IP address space.

## Follow the principle of least privilege

If the SamSam attackers gain access to your network they will try to become Domain Administrators using a combination of hacking tools and exploits.

One approach uses the credential harvesting tool Mimikatz to steal a Domain Administrator's password from memory when they log in.

Privilege escalation can take days and the longer it takes, the more chance you have of spotting the intruder. To contain and frustrate an attacker you should follow the principle of least privilege, giving user accounts only the access rights they need and nothing more. For example:

- Users who don't need to install software should not have administrative privileges.
- Domain Admin accounts should be used for administration tasks, not for mail or web browsing.
- Where possible, favour elevating to domain privileges over the use of Domain Admin accounts.
- Don't give service accounts for important services like SQL databases access to backups.
- Restrict access to critical system to the smallest possible group.
- Lock down access to C$ and other shares as much as possible.

You may find models or approaches to privileged access, such as Microsoft's tiers-based approach, useful, as well as tools like BloodHound that can help you identify and eliminate hidden risks.

The principle of least privilege applies to software as well as access.

The extensive use of administration tools such as PowerShell, PsExec and PAExec, and of Potentially Unwanted Applications like Mimiktaz, during attacks makes the proper configuration of application control technologies vitally important.

Scripting languages such as JavaScript and Powershell, and admin tools like PsExec, should be blocked everywhere they aren't needed, or blocked everywhere and allowed as and when they're required.

The SamSam technical details section of the research contains more information about the software that's been seen in SamSam attacks.

### Assume an attack is a matter of ‘when’, not ‘if’

When you’re considering your defence against SamSam it’s important to remember that the execution of the actual SamSam ransomware is the final step in the attack. Up to that point you are dealing with a skilled intruder who may be able to exercise tremendous power on your network, and who can counter your defensive moves.

You cannot wait until after you’re breached to determine what you’ll need or what you should do, by then it’s too late. To prepare accordingly, you must act as if it’s a matter of *when you’re breached*, not *if you’re breached*.

You will need to have trained and well drilled staff and software capable of monitoring and reacting to anomalous events on your network, such as unusual account activity, in real time.

Careful selection of software with the right approaches to automation, reporting and interoperability is important.

Its reporting capabilities, and its ability to talk to other security software, should ensure your staff have sufficient, relevant information, but aren’t overwhelmed.

Automation is important because SamSam malware is designed to act quickly, and to encrypt your most important files first. It’s typically launched in middle of the night or the early hours of the morning in a victim’s local time zone, when most users and admins are asleep.

## What if an attack is successful?

Should a SamSam attack successfully encrypt computers on your network you’ll need to be able to get back up and running quickly, and understand what you need to do to prevent it happening again.

Unlike most other ransomware, SamSam doesn’t just target document files and data, it also targets applications and configuration files. So, before you can restore your data you’ll need to reinstall or reimage your computers’ operating systems and applications, and that can take a long time if you aren’t prepared for it.

When looking at your SamSam-resistant backup strategy it’s useful to consider the same questions you might face in the event of a fire or flood, like: how many computers does your organisation need to maintain a bare-bones operation, how long would it take to restore those machines, and how long would it take you to return to normal operations?

You don’t want to find yourself in the position of having survived an attack but paying the ransom anyway because you can’t restore your computers fast enough.

Similarly, you must remember that if a Domain Administrator on your network can access your backups then an attacker acting as a Domain Administrator one can destroy or encrypt them.

Therefore, your backup strategy should:

1. Account for how you will restore the necessary number of entire machines, not just data.
2. Include offline and offsite backups that put an air gap between them and an attacker.

Should the worst happen you'll also want to have collected enough information for a retrospective analysis that can answer questions like: what was lost, how did the attacker get in and how can you prevent it happening again?

## Further reading

You can read more about the history of SamSam, how it works and how to protect against it in Sophos's extensive new research paper, **SamSam: The (Almost) Six Million Dollar Ransomware**.

The investigation is ongoing – if you have information about SamSam or you are a security vendor interested in collaborating with our investigation, please contact Sophos.