SamSam: The (almost) $6 million ransomware

nakedsecurity.sophos.com/2018/07/31/samsam-the-almost-6-million-ransomware/

By Mark Stockley 31 Jul 2018

Extensive research by Sophos has uncovered a trove of new information on the notorious SamSam ransomware, revealing that it has affected far more victims than previously thought, and raised vastly more in ransom demands – almost $6 million.

Through original analysis, interviews and research, and by collaborating closely with industry partners and a specialist cryptocurrency monitoring organisation, Sophos has uncovered new details about how the secretive and sophisticated SamSam ransomware is used, who's been targeted, how it works and how it's evolving.

A different breed of malware

What sets SamSam apart from most other ransomware, and why detailed research about it is so important, is the way it's used in stealthy, targeted attacks.

Most ransomware is spread in large, noisy and untargeted spam campaigns sent to thousands, or even hundreds of thousands, of people. They use simple techniques to infect victims and aim to raise money through large numbers of relatively small ransoms of perhaps a few hundred dollars each.

SamSam is very different – it's used in targeted attacks by a skilled team or individual who breaks into a victim's network, surveils it and then runs the malware manually. The attacks are tailored to cause maximum damage and ransom demands are measured in the tens of

thousands of dollars.

Because the malware has been used so sparingly compared to other types of ransomware, details about how it works and how the attacks play out have been elusive since its first appearance in December 2015.

Although you are unlikely to be the target of a SamSam ransomware attack – attacks occur at a rate of about one per day – those who are can find the effects devastating.

New insights

The research paper reveals a host of fresh technical insights including new details about how SamSam scans victims' networks and builds up the list of machines it's going to encrypt.

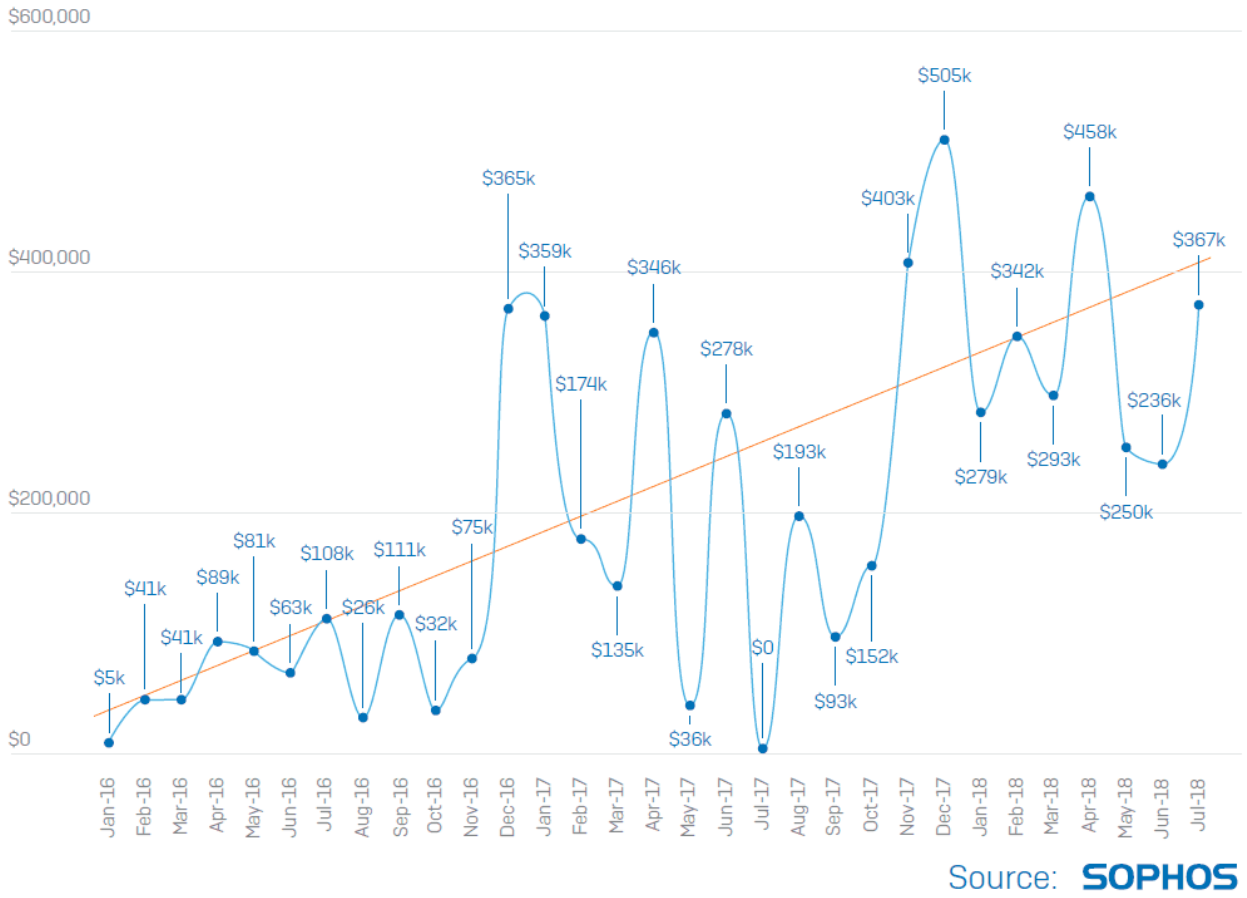
Perhaps most eye-catching though is new information about how it spreads: Unlike WannaCry, which exploited a software vulnerability to copy itself to new machines, SamSam is actually deployed to computers on the victim's network in the same way, and with the same tools, as legitimate software applications.

Sophos's investigation also sheds new light on the number of attacks, how often they occur and who has been targeted.

Based on the known victims, it's been widely speculated until now that SamSam attacks are directed specifically at the healthcare, government and education sectors. Sophos can reveal that this is not the case.

Working with cryptocurrency monitoring organisation Neutrino, Sophos followed the money and identified many ransom payments and victims that were previously unknown. Based on the much larger number of victims now known it seems that far from being unaffected, the private sector has actually borne the brunt of SamSam. Victims in that sector have simply been far more reluctant to come forward.

The money trail also revealed that SamSam has netted nearly $6 million in ransom payments – about six times more than the most recent best estimate.



From its new research, Sophos is also able to offer better protection and disaster recovery advice too. Thanks to an improved understanding of the way that SamSam targets files in the victim's operating system, Sophos now recommends that backing up your business data is not enough. To recover swiftly from a SamSam attack, organisations need more than a plan for restoring data – they need a comprehensive plan for rebuilding machines.

How attacks unfold

The SamSam attacker gains access to victims' networks via RDP (Remote Desktop Protocol) by using software like nlbrute to successfully guess weak passwords.

Sophos has identified that the timing of attacks changes to reflect the victim's timezone. Whether the victim is on the west coast of the USA or in the UK, attacks happen at night time while the the victims are asleep.

Unlike other well-known ransomware such as WannaCry or NotPetya, SamSam doesn't have any worm-like or virus capabilities, so it can't spread by itself. Instead, it relies on the human attacker to spread it – an attacker who can adapt their tactics according to the environment and defences they discover as they surveil the target.

By working in this way, the attacker can try over and over again to work around defences and gain the access they want. If the SamSam attacker is on your network they will likely stay on it until they succeed, unless they're kicked off.

Having gained access to a network, the SamSam operator uses a variety of tools to escalate their privileges to the level of Domain Admin. Then they scan the network for valuable targets and deploy and execute the malware as any self-respecting sysadmin might, using utilities such as PsExec or PaExec.

Once it has been spread far and wide, the many copies of the ransomware are triggered centrally, starting within seconds of each other. On each infected machine, files are encrypted in a way that's designed to cause the most damage in the shortest time.

Once the attack has been launched, the attacker waits to see if the victim makes contact via a Dark Web payment site referenced in the ransom note.

Ransom demands have increased over time to about $50,000, vastly more than the three figure sums typical of untargeted ransomware attacks.

What to do?

To avoid becoming a victim, the best defence against SamSam or any other form of malware is to adopt a layered, defence in depth approach to security.

SamSam targets appear to be chosen on the basis of their vulnerability. Earlier attacks established a foothold on victims' networks by exploiting known software vulnerabilities. More recently the attacks have begun with the brute forcing of RDP credentials.

Staying on top of your patching and maintaining good password discipline will therefore provide a formidable barrier to SamSam attacks. That barrier can then be strengthened significantly with these simple steps:

1. Restrict RDP access to staff connecting over a VPN.
2. Use multi-factor authentication for VPN access and sensitive internal systems.
3. Complete regular vulnerability scans and penetration tests.
4. Keep backups offline and offsite.

Of course SamSam is just one of millions of cyberthreats and this detailed examination of SamSam is just part of the constant, ongoing malware research undertaken by Sophos to improve and adapt its ability to protect against all forms of malware.

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.