SOPHOS
Cybersecurity made simple.

SamSam: The (Almost) Six Million Dollar Ransomware

After hundreds of hours of extensive research by SophosLabs, including original analysis, interviews, research, and more, and working side by side with cryptocurrency monitoring organization Neutrino, we have discovered that the notorious SamSam ransomware has caused far more harm than previously thought – totaling upwards of $6 million.

SophosLabs has uncovered a trove of information about the ransomware, which uses secretive, targeted attacks that differ from the splashy, messy, but effective methods large-scale ransomware attacks use. Rather than stealing money through many, many small transactions over a vast number of victims, SamSam uses targeted attacks by a skilled team or individual, causing maximum damage by tailoring the attack to each victim, with ransom demands in the tens of thousands of dollars.

SamSam has remained elusive, used stealthily and sparingly compared to over headline-grabbing ransomware attacks, undergoing several key evolutions over time. It is a very different sort of ransomware, used roughly once per day in one devastating, handcrafted attack.

The following paper reveals a host of new information on SamSam, examining how it works, how its spreads, how widespread it is – and why we have not, until now, known just how large an impact SamSam has had. We also follow the money, discovering previously unknown victims and payments. Lastly, we'll discuss what you and your organization can do to guard against this sort of tailor-made, targeted attack.

Introduction

As the year 2016 began, a ransomware threat appeared that attacked its victims unlike any previous ransomware attack. SamSam, named after the filename of the earliest sample we uncovered, uses a brutally minimalist, manual approach to target and compromise victims.

The attacker or attackers use a variety of built-in Windows tools to escalate their own privileges, then scan the network for valuable targets. They want credentials whose privileges will let them copy their ransomware payload to every machine – servers, endpoints, or whatever else they can get their hands on.

Once in, the attacker(s) spread a payload laterally across the network; a sleeper cell that lays in wait for instructions to begin encrypting. Ever a predator, the attacker waits until late at night, when the target organization is least well equipped to deal with it, before the final blow is struck. A sneak attack while the target literally sleeps, SamSam encrypts a prioritized list of files and directories first, and then everything else.

Unlike virtually every other ransomware attack, the entire attack process is manual. No badly worded spam email with an attachment is the culprit. The attacker breaks in the old-fashioned way: using tools that attempt as many logins as quickly as the Remote Desktop Protocol will permit, and exploits operating system vulnerabilities, though not as many as you'd think. SamSam usually succeeds when the victim chooses a weak, easily guessed password.

Key Findings

- SamSam has earned its creator(s) more than US$5.9 Million since late 2015.
- 74% of the known victims are based in the United States. Other regions known to have suffered attacks include Canada, the UK, and the Middle East.
- The largest ransom paid by an individual victim, so far, is valued at US$64,000, a significantly large amount compared to most ransomware families.
- Medium to large public sector organizations in healthcare, education, and government have been targeted by SamSam, but our research discovered that these only make up for about 50% of the total number of identified victims, with the rest comprising a private sector that has remained uncharacteristically quiet about the attacks.
- The attacker uses care in target selection and attack preparation is meticulous. SamSam waits for an opportune moment, typically launching the encryption commands in the middle of the night or the early hours of the morning of the victim's local time zone, when most users and admins would be asleep.
- Unlike most other ransomware, SamSam encrypts not only document files, images, and other personal or work data, but also configuration and data files required to run applications (e.g., Microsoft Office). Victims whose backup strategy only protects the user's documents and files won't be able to recover a machine without reimaging it, first.
- Every subsequent attack shows a progression in sophistication and an increasing awareness by the entity controlling SamSam of operational security.
- The cost victims are charged in ransom has increased dramatically, and the tempo of attacks shows no sign of slowdown.

The Anatomy of a SamSam Attack

SamSam attacks follow a relatively predictable pattern, and usually comprise of the following six stages.

1. Target identification and acquisition
2. Penetrate the network
3. Elevate privileges
4. Scan the network for target computers
5. Deploy and execute ransomware
6. Await payment

SamSam has evolved through three major versions since its inception, as well as a number of smaller changes, most of which involve pragmatic procedures: the payment sites, ransom notes, and the extensions added to encrypted files.

For example, while the attacker has always used a website to arrange payment of the ransom, during the beta testing phase, the SamSam attacker(s) used websites hosted on anonyme.com, which (at the time) was an anonymous hosting service. The attackers switched to using free and anonymous WordPress sites once they released version 1, but after a couple of months, they moved to the dark web and hosted the payment sites on Tor .onion addresses.

Since the earliest versions of SamSam, the ransom notes left behind on the victim's network after an attack have been unique to each victim. The bulk of the ransom note content has remained the same throughout, however for all of 2016 and most of 2017, victims were provided a unique URL for their payment site, as well a new Bitcoin address to send any ransom payments to.

When version 3 of SamSam was released, everything changed. Version 3 had the most features designed to protect the integrity of the software and to help obfuscate the attacker's identity.

The change to version 3 also saw smaller changes, such as to the filenames of the ransom notes, and to the file extensions appended to encrypted files. The encrypted files have always followed the same naming convention of appending a new extension to the end of an encrypted file. But with the change to SamSam version 3, the attacker has struck a more apologetic, contrite tone with a ransom note.

These changes, and the fact that there is more consistency in the naming of files seen in SamSam attacks, is partly why we think there has been more media coverage of SamSam in 2018. It is now easier for researchers to link attacks back to SamSam.

Since the end of 2015, SamSam has evolved to focus on two main objectives: First, to improve the deployment method so that the impact on victims is greater; Second, to make analysis of the attacks harder, further helping to keep the attacker's identity a secret.

Identifying the Victims?

SamSam has made headline news for its attacks on organizations in the healthcare, government, and education sectors. There is no denying that SamSam have hit some very high profile targets organizations we believe have been victims of SamSam, and it's the private sector who have suffered the most (and disclosed the least) The reason that the healthcare, government and education sectors dominate the headlines is simply because they have been, so far, more likely to go public about a SamSam attack than any companies in the private sector.

Based on our research of the Bitcoin addresses in ransom notes, we estimate that about 233 victims have paid a ransom to the attacker, but we don't know the identities of all those victims. In this paper, we do not provide details of those victims who have chosen to keep information about an attack private, instead only referring to the countries that they are in, and their broad industry sectors.

Sophos has determined that 74% of the victim organizations identified are based in the United States. In terms of industries:

- Private Sector: 50%
- Healthcare: 26%
- Government: 13%
- Education:11%

Using these victims as our baseline, we looked at how many went public about the attack. It is worth noting that many of those who did go public did not specifically mention SamSam, or even ransomware. The organizations often referred to the attack as an "incident" or referenced generic "computer problems," without identifying the root cause. Only through our research and working with other security vendors were we able to separately confirm it was SamSam.

Percentage of SamSam victims by sector that went public:

- Government: 100%
- Healthcare: 78%
- Education:38%
- Private Sector: 0%

Tracking the Money

During Sophos' investigation into SamSam, we identified a number of Bitcoin addresses supplied on ransom notes and in sample files. This allowed us to track all the ransom payments made to these addresses.

But to advance the investigation, Sophos teamed up with Neutrino, a firm who specialize in developing "solutions for monitoring, analyzing, and tracking cryptocurrency flows across multiple blockchains, providing actionable insight on the whole cryptocurrency ecosystem." With their assistance, we have been able to identify further Bitcoin addresses used in SamSam ransomware attacks.

In total, we have now identified 157 unique addresses which have received ransom payments as well as 89 addresses which have been used on ransom notes and sample files but, to date, have not received payments. According to Neutrino, the addresses which have received payments can be grouped into three Bitcoin wallets, each controlled by one owner. These same three wallets have been used by the attacker since the SamSam attacks began.

Since 2016 multiple security vendors have published articles on the topic of SamSam and several estimates have been made as to how much money has been earned by the attacker. The highest estimate has been US$850,000. Unfortunately, all the estimates to date fall short of the reality. Thanks to the research by Sophos and Neutrino we have now confirmed the true number to be more than US$5.9 Million, with the average monthly take currently standing at around US$300,000.

Identifying SamSam's Creator/Operator

As of the date of this publication, the identity of the author behind SamSam remains unknown. Unlike some cyber criminals, the author of SamSam is not known for bragging about their exploits on Twitter or dark web forums. As described in the Technical Details section of this paper, they invest a lot of effort into covering their tracks and remaining anonymous. Based on Sophos' research, combined with information provided by other vendors, we can make the following observations:

The consistency of language across ransom notes, payment sites, and sample files, combined with how their criminal knowledge appears to have developed over time, suggests that the attacker is an individual working alone. This belief is further supported by the attacker's ability not to leak information and to remain anonymous, a task made more difficult when multiple people are involved.

The attacker's language, spelling and grammar indicates that they are semi-proficient in English but they frequently make mistakes.

In terms of grammar, there are other tics and tells. For instance, the attacker regularly capitalizes the word immediately following a comma, as if the comma was a period. This characteristic error appears in both the ransom notes and in comments the attacker keyed into the payment site chat feature, and the hypothesis that "SamSam" may be the work of just one person.

Timing for maximum effect

In almost every attack, the attacker started encryption of files late at night or in the early hours of the morning, in the victim's time zone. There is a sort of twisted logic to this, as this will be a time when victims are most vulnerable, as there are likely to be fewer users and admins online to notice. This is true of US victims both East and West coast as well as victims in other countries such as the UK.

Reviewing the metadata of around 200 sample executables used in attacks, and more specifically the timestamps of these files, we can gain an insight into the attacker's working pattern. Of course, timestamps can be faked but we do not believe this to be the case.

We found that 94% of the samples were compiled in a 16-hour window starting at 9 a.m., going through to 1 a.m. that night, leaving an eight-hour window where we assume the attacker is sleeping.

We can see that the attacker has a toolkit of hacking applications and malicious files which are kept-on hand for use in attacks. The attacker appears to create a stockpile of the malware payloads, sometimes weeks in advance, so if a sample is stopped by antivirus, the attacker can quickly switch to a newer sample and continue to press the attack.

For most attacks, the attacker will use tools and malicious files which have been used in previous successful attacks.

When launching an attack, if some of the files are detected by the incumbent antivirus, the attack may be interrupted. In the event of this first wave effectively failing, the attacker will switch to using different tools and newer malicious files from their stockpile to launch a second wave of the attack.

This second wave may begin hours or even days later. While this method's manual approach seems quaintly antiquated, it does increase the chance of a successful attack. However, it also provides the victim with an opportunity to identify an attack taking place. If a victim, through human intervention or automated security systems, can act on this information, it might be possible to remove the attacker's access to the network before a second wave is launched.

In summary, while we know a lot about how the attacker works and can make some interesting observations, what is clear is that they have remained anonymous for over two and a half years and continue to show signs of their attacks becoming more sophisticated.

How to Stay Protected

Securing an environment against a competent, persistent, and patient, human adversary is somewhat different from defending against the more conventional kinds of semi-automated, social engineering-driven threats more commonly seen in enterprise environments. And SamSam's own particularly damaging behavior sets it apart from many other ransomware.

There are four specific, immediate steps you should take to defend against SamSam:

1. Restrict access to port 3389 (RDP) by only allowing staff who use a VPN to be able to remotely access any systems. Utilize multi-factor authentication for VPN access.
2. Complete regular vulnerability scans and penetration tests across the network. If you haven't followed through on recent pen-testing reports, do it now.
3. Multi-factor authentication for sensitive internal systems, even for employees on the LAN or VPN.
4. Create backups that are offline and offsite and develop a disaster recovery plan that covers the restoration of data and whole systems.

Real-time network and event monitoring is also a key component of prevention, as these kinds of tripwires may be able to catch and halt the break-in in the act – behavior that may not, immediately, appear to be malicious. In our experience, endpoint protection is also crucial but shouldn't be the first line of defense; A reactive human adversary prepared to deploy new, unique malware specifically to bypass endpoint AV is a tough nut to crack.

We recommend you also follow these more general tips for staying safe:

Reduce the organization's threat profile to avoid being an easy target. Diligently keep machines up to date, use strong passwords, two-factor authentication, and patch regularly.

Follow the **Principle of Least Privilege**, giving users and admins the least amount of access rights they need to do their job.

Have **security solutions in place** that can detect advanced threats and communicate with your firewall to restrict access to affected computers.

Follow **basic security measures** like determining if you want your users to be able to execute JavaScript and Powershell; whether you need domain admin accounts; lock down access to the c$ and other shares on every computer; restrict access to departments appropriately; ensure powerful administrative tools are not authorized on every computer.

Monitor your environment and look for anomalies. Because of the unconventionally manual nature of SamSam's attack method, in which a skilled threat actor is countering your defensive moves as they happen, real-time monitoring for anomalous events may be the only real way of truly preventing harm.

Perform retrospective analyses after attacks to learn the answers to how did the attacker get in," "what did I lose," and "how can I be sure this won't happen again?" You can't ever know the answer to those questions later if you're not collecting the information that could lead you to them, now.

Summary

SamSam poses a severe though manageable threat to organIzations globally, despite the fact that the majority of victims thus far have been based in the US. Whilst the media has reported numerous high-profile attacks on hospitals and government bodies, it is, in reality, the private sector that is being targeted the most. Since the first attacks, SamSam has only grown in sophistication and has become more prolific. SophosLabs estimates that the attacker's revenue from ransom payments now averages around US$300,000 per month.

One reason SamSam enjoys outsized success rates is down to the combination of tools and tactics that the attacker employs. The use of legitimate services such as RDP and tools such as PsExec allows the attacker to take advantage of weaknesses in organIzations' environment's without having to create malicious files, which are more easily detected. Additionally, the attacker (believed, but not proven to be one person) is thorough and consistent in covering their tracks and making analysis difficult.

Whilst an attack which has been specifically crafted for its target, is more difficult to prevent than the more commonplace fire and forget malware, it is possible to prevent such attacks.

Sophos recommends that organIzations adopt a layered security approach for networks and devices, both to reduce an organIzation's attack surface and attractiveness to attackers, and in the event of penetration, to block the attacker at every opportunity. A security solution, containing systems which automatically communicate with one another to identify and respond to current threats, is the best approach to protecting your organIzation.

For more information on ransomware visit: www.sophos.com/ransomware

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2018-08-06 DS-NA (MP)

SOPHOS