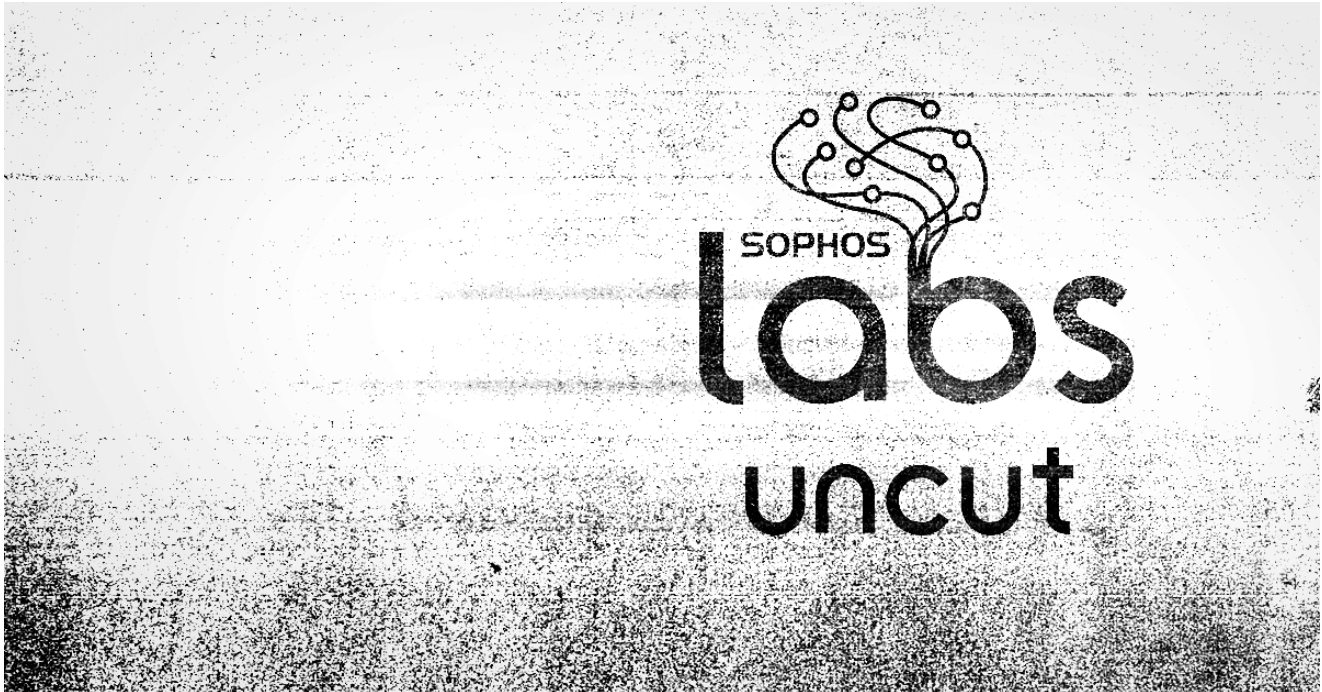


How a SamSam-like attack happens, and what you can do about it

news.sophos.com/en-us/2018/11/29/how-a-samsam-like-attack-happens-and-what-you-can-do-about-it/

Andrew Brandt

November 29, 2018



By Andrew Brandt

The threat actors behind the SamSam ransomware, now identified by the FBI in an indictment (and [very fancy Most Wanted poster](#)), pioneered a very specific playbook in their attacks that has inspired a rash of copycats. In July, we published [a report that goes into great detail](#) about the SamSam TTP, so if this is of interest to you, maybe check it out. Here's a quick explainer of their TTP (tactics, techniques & procedures) and some easy countermeasures you can enact today.

- Target identification
 - “Can the target pay?”
- Penetrate the network
 - Brute force RDP
 - Targeted exploits (JBOSS)
- Elevate privileges
- Scan internally for targets
- Deployment & execution
- Sit back and wait for the victims to come to you

Summary of the attack

procedures used by SamSam

The SamSam attackers started by conducting surveillance of the victims. They wanted to know if the victims had sufficiently deep pockets to pay the ransom, which over time averaged out to the mid-\$30,000 as Bitcoin exchange rates fluctuated.

Step 1: Target acquisition

- Not a lot of information
 - Medium- to large-sized orgs and enterprises
- No honor among these thieves
 - Indiscriminate target choices
 - Victims include a homeless charity, schools, hospitals, orgs with ability to pay but that other criminals seem to avoid
- May be using [Shodan](#), [Censys](#), NMAP, Kali, to scan
- Most targets in the US, majority in the “Anglosphere”



SamSam

SOPHOS

target acquisition

In fact, the surveillance may have used a number of freely available tools, but the primary motives seem to be (1) whether the victims were based in the “Anglosphere” (English-speaking world, but primarily in the US) and (2) had money, and that’s it. Some ransomware attackers appear to have avoided attacking schools or hospitals, but not SamSam.

- “Low hanging fruit”
 - Most victims have had unprotected RDP and poor password policies
 - [NLBrute](#) brute forcing RDP tool
 - [xDedicRDPPatch](#) – creates RDP accounts
 - [RDPWrap](#) – Allows simultaneous local & remote login
 - Some (especially earlier) victims were running vulnerable JBOSS servers
 - “[JexBoss](#)” tool for exploitation

employed by SamSam during the intrusion phase of the attack

The attackers relied on “low-hanging fruit” to break in to networks. Most attacks begin with the attackers brute-forcing passwords for Windows machines that have [Remote Desktop Protocol](#) (RDP) exposed through a hole in the firewall.

If you have ports open in your firewall to let RDP through from the internet, and it isn't behind a VPN, **please close those ports now**. It doesn't matter how strong the Windows password is. It is **not worth the risk** to keep it open.

Some early attacks began with exploits against vulnerabilities in a application service called JBOSS (now known as [Wildfly](#)). The attackers use a publicly available grey-hat hacking tool called [JexBoss](#). An IoC of this type of attack is the file [jbossass.war](#) (MD5: [CBDEAF83F58A64B09DF58B94063E0146](#)). This method quickly fell out of favor in lieu of using RDP.

- Sysadmin & grey hat tools
 - [Mimikatz](#) – used to capture Domain Admin creds
 - [reGeorg](#) – SOCKS proxy with TCP tunneling and net analysis
 - [Hyena](#) – AD remote admin tool
 - [WMIexec/PAExec](#) – executes commands through WMI
 - [csvde.exe](#) – AD Lightweight Directory Services data mgmt. tool

SamSam use conventional systems administration and some grey-hat hacking tools

Once the SamSam attackers gained a foothold in the network, they used a variety of grey-hat and systems administrator tools to escalate their own privileges. The goal: Obtain Domain Administrator credentials, usually by sniffing for them using Mimikatz.

- Take control of Domain Controller
- Attempts to write a plaintext file named test.txt to targets
 - If successful, target is added to a list called alive.txt on DC

The goal was to take control of the Domain Controller

As soon as they had the Domain Administrator password, the SamSam attackers took control of the Domain Controller. They leveraged the DC to distribute the ransomware to every machine on the network, but they didn't do it right away. They did tests first, before deployment, to make sure the DC has write privileges to the machines under its bailiwick.

- Uses Sysinternals PsExec (or PaExec) to deploy
 - Advantage: manual attacker can change methods on the fly
 - Lots of sanity checking built into the process
- Attacker waits until the **WORST** possible time to strike
 - Late at night at victim's location; on weekends; over holidays

SamSam pushed an installation using the free Microsoft Sysinternals tool PsExec. Using Microsoft's free tool PsExec, the attackers pushed ransomware to every machine they could reach from the DC, all at once.

They waited until late at night, over weekends, or holidays to launch the attack, when the fewest people might notice before it was too late.

In cases where an endpoint security product was preventing the malware from running, they taught themselves how to use the administrator consoles that enterprises use to manage security products, and would selectively disable security products using (you guessed it) stolen admin credentials.

At the very least, **administrator-level users must use two-factor authentication for all sensitive services and accounts.**

```
psexec -accepteula -s \\machine-name cmd.exe /c if exist  
C:\windows\system32\g04inst.bat start /b g04inst.bat <PASSWORD>
```

The PsExec command launched a batch file and required a password, which makes analysis harder.

To make it harder for security experts to analyze the malware, they built samples unique to each victim organization, and executed them using a batch file that decrypted the payload with a password they changed for each attack. The malware always deleted its own installer and any other traces as a final step. Getting copies of the files associated with the attack has been a challenge since the earliest days, but it wasn't impossible.

Prioritization of hostile encryption

- SamSam does not just encrypt documents, images, etc.
 - Everything not required for Windows to run gets hit
 - Applications, config files, large databases
- For maximum efficiency and impact, it prioritizes its activity
 - Starts by encrypting all files with specific extensions
 - If a file is locked, it kills the process locking the file
 - Next it encrypts all the rest of the files (that aren't on an exclusions list), starting with the smallest and working up to the largest
- Generates a unique AES key and IV for each individual file
 - Prepends these to each encrypted file
- Wipes out evidence, traces, the second encryption is complete

SOPHOS

The SamSam attackers refined the encryption procedure many times over two years. The SamSam ransomware pushed the limits for efficiency, too. It encrypted the most important files first, and then *everything else* that wasn't essential to keeping the machine running.

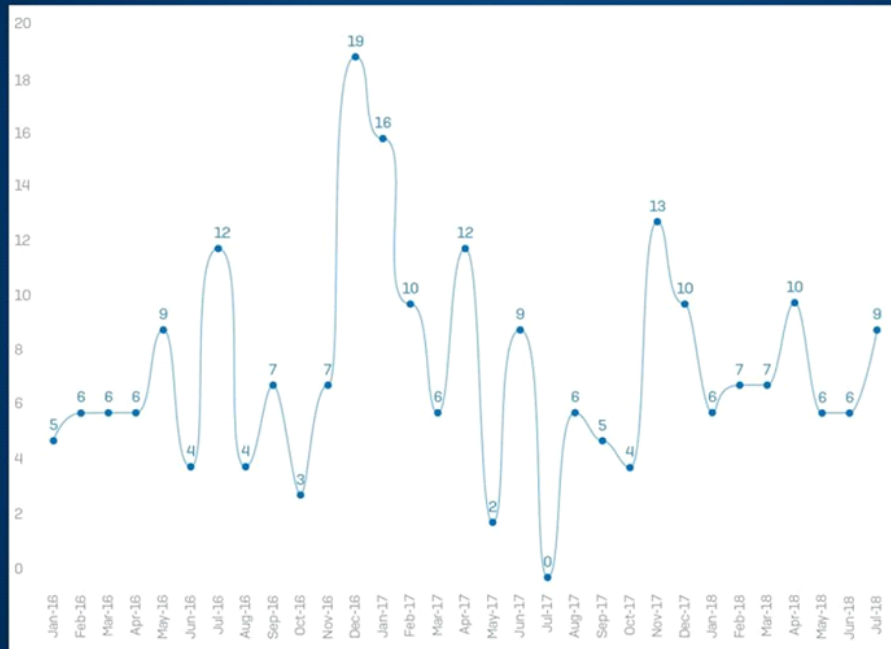
The consequences were more serious than with conventional ransomware. For instance, you couldn't just restore data files from backups to get back up and running, because **all your applications are also inaccessible**. You need to reimage the disk first, and restore all the applications, before you could restore the data files.

It was a purely evil act and virtually guaranteed that data was unrecoverable in a reasonable amount of time at the scale of whole networks, all at once. If it took (just for example) 30 minutes to reimage a disk on a single machine, and another 15 to bring back the data from offline backups, how long would it take to do the same on 100 machines? How about on 1000 machines?

Could you do this for a massive global organization quickly enough not to incur heavy losses? What if you weren't just a gaming network and lives literally were hanging in the balance?

Faced with a prospect of, perhaps, weeks of downtime and painstaking recovery, and the ensuing lost productivity, it's not surprising so many victims opted to pay the SamSam attackers. For many, it was a matter of organizational survival, though a costly lesson to learn.

Number of paying victims per month (estimate)



SamSam only attacked a handful of organizations at a time, but had a high success rate. Every victim was provided with a unique .onion address on the dark web. At the other end, there was a kind of chat system where the victim interacted directly with the SamSam attackers.

Time Played: 1 days 20 hours 6 minutes 35 seconds

Please wait for decrypt files

Upload File For Decryption

Files Available To Decrypt: 0

| Your comments | Our Answer |
|--|---|
| 27.09.2016 08:02 --[REDACTED]@gmail.com hello there, I am not sure it worked there seem to be some systems it didnt work on can you check if there are any more keys please? thank you | all keys: You can download it from address: http://s000.tinyupload.com/?file_id=[REDACTED] You can delete file from address: http://s000.tinyupload.com/?del_id=[REDACTED] |
| 27.09.2016 12:08 --[REDACTED]@gmail.com an error occured when decoding OAEP padding value cannot be null parameter name: yek is the error we see after the tool has been running some time around 1/4 files are restored, the rest fail with this error thank you for your help | What error did you get? It was all of your keys Padding Error most occur for files in shared folder because they are used in many computers and some files encrypted with another computer key. |
| 27.09.2016 13:26 --[REDACTED]@gmail.com ok, how do you think we can fix? thank you | fixing is a little boring, You should find undecrypted file that send you error, copy this file to a new PC, now copy all keys in the next to of unencrypted file, now you should write a batch file that select key one by one and start decrypting. |
| 27.09.2016 13:30 --[REDACTED]@gmail.com ok, how do you think we can fix? thank you | |

SamSam's attackers communicate with victims through a bespoke dark web chat page

These disappeared as soon as the victim paid. Only a few screenshots exist. This one was shared with us by a victim who worked with us to investigate the attack retrospectively.

We tracked Bitcoin payments to a small number of wallets. The cryptocurrency was then “tumbled” to obfuscate its origin and destination.

Tracing payments is hard

- Attacker transfers to multiple accounts the same day
- Attacker doesn't transfer until all ransom is received
- Multiple ways to “launder” cryptocurrency
 - Put the coins into a “tumbler” service
 - Convert Bitcoin to another type, such as [Monero](#)
 - Use of “mixers” – substitute Bitcoin for other currency types never used on dark markets ([Helix](#) or [Bitmixer](#))
- [SamSam](#) attacker has used all three methods

SOPHOS

The attackers laundered their Bitcoin through “tumbler” services

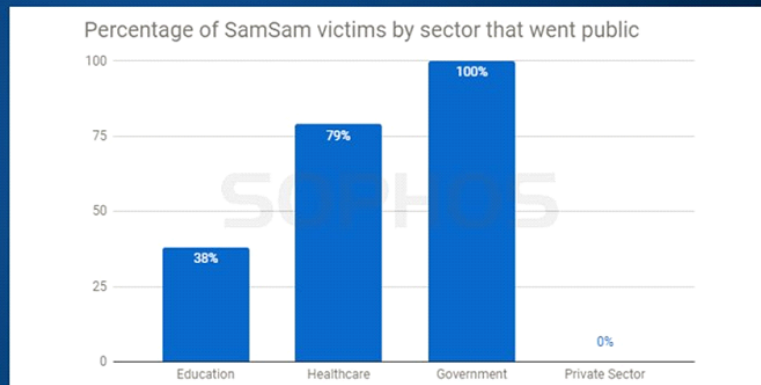
We traced many of these back to their origins and found something quite interesting

While many victims, including the [City of Atlanta](#), openly admitted they had been targeted by SamSam, more than half of the paying victims never made any kind of public announcement at all.

Who are these silent victims?

- Variety of business sectors, about half of the estimated victims

- Energy
- Financial services
- Manufacturing
- Logistics
- Legal
- IT and technology
- Construction
- Media
- Public transportation
- Nonprofits and charities



More than half the SamSam victims never made a public announcement about the attack. All these “silent victims” were large businesses.

It’s also clear that the SamSam attackers had a single country primarily in their crosshairs, once you correlate the victim organizations’ location.



Data from January 2016 to July 2018, including “silent victims”

Now that we know who the attackers were, the motivation seems kind of obvious.

The news about the FBI identifying and indicting the SamSam threat actors makes us happy, but it doesn't mean the case is closed. Far from it, in fact.

Nobody's been arrested, and there is still a lot of low-hanging fruit out there.

Worse, several other threat groups have picked up on this modus operandi, and are mimicking the SamSam technique to spread ransomware. These white-glove, hand delivered, targeted attacks are still going on.

Reducing your threat profile

- Close ALL access to RDP (3389/tcp) from outside the firewall
 - This does not include VPN
- Enact and enforce good, complex password policies
 - Don't trust, verify
 - Use multifactor authentication
- Periodic assessments of your own network
 - Start by looking at both [Shodan](#) and [Censys](#)
 - Identify publicly-accessible ports/protocols
- Patch, patch, patch, patch, patch! Then check and patch again!

SOPHOS

So, we all have a lot of work to do. This fight is only entering the next phase. Close those RDP ports! Patch your old boxes! Segment the network so everything can't be reached from a single point. At the very least, pick your low hanging fruit and make some fruit salad!

We'll be covering the rise of targeted ransomware and its aftermath, right here in our SophosLabs blog. Join us as we fight this scourge!



WANTED BY THE FBI

SAMSAM SUBJECTS

**Conspiracy to Commit Fraud and Related Activity in Connection with Computers;
Conspiracy to Commit Wire Fraud; Intentional Damage to a Protected Computer;
Transmitting a Demand in Relation to Damaging a Protected Computer**



Mohammad Mehdi
Shah Mansouri



Faramarz Shahi Savandi