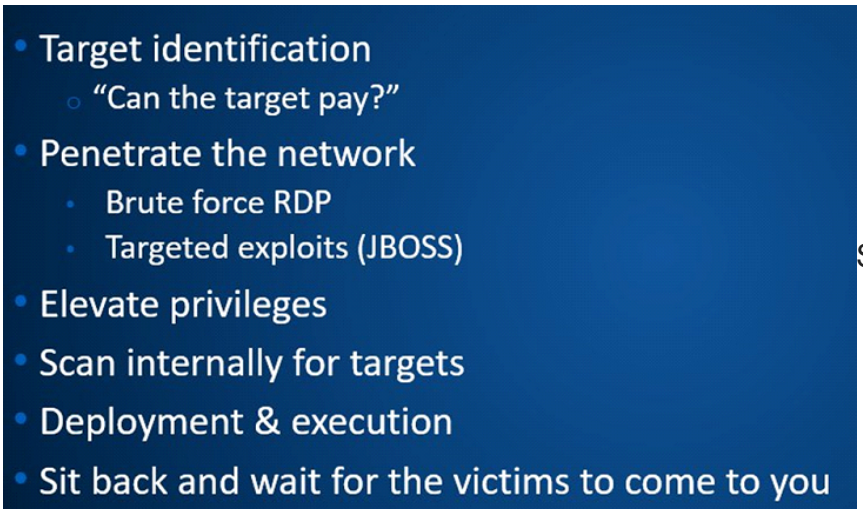
How a SamSam-like attack happens, and what you can do about it

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

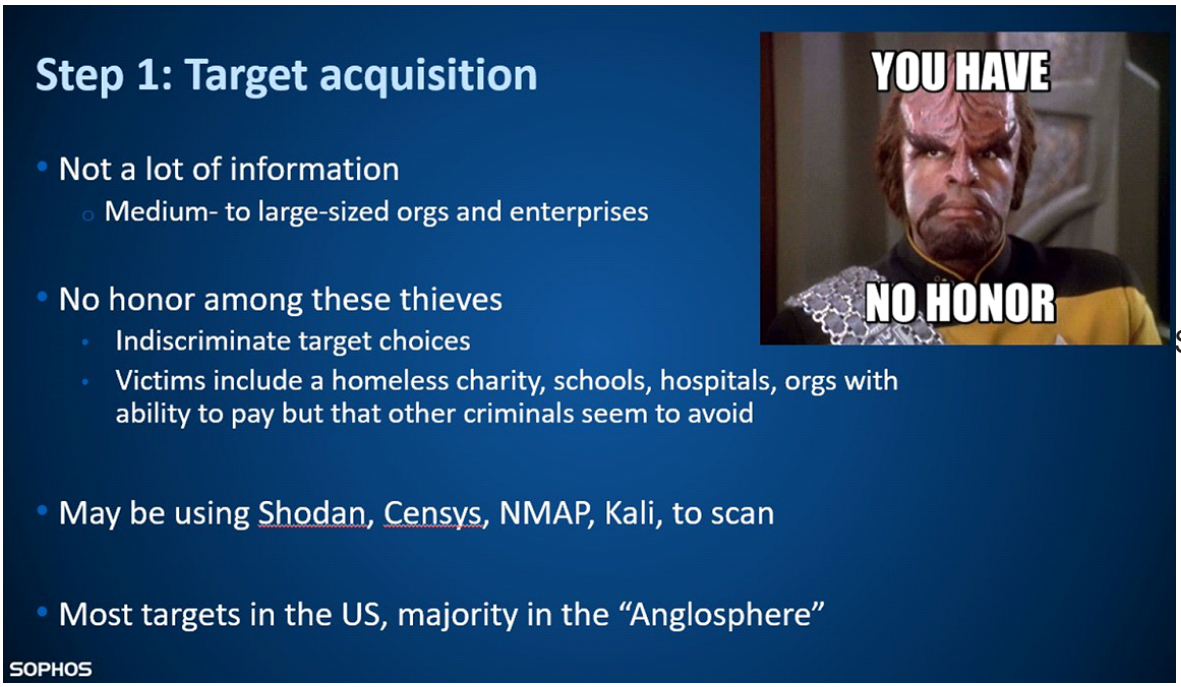
By Andrew Brandt

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.



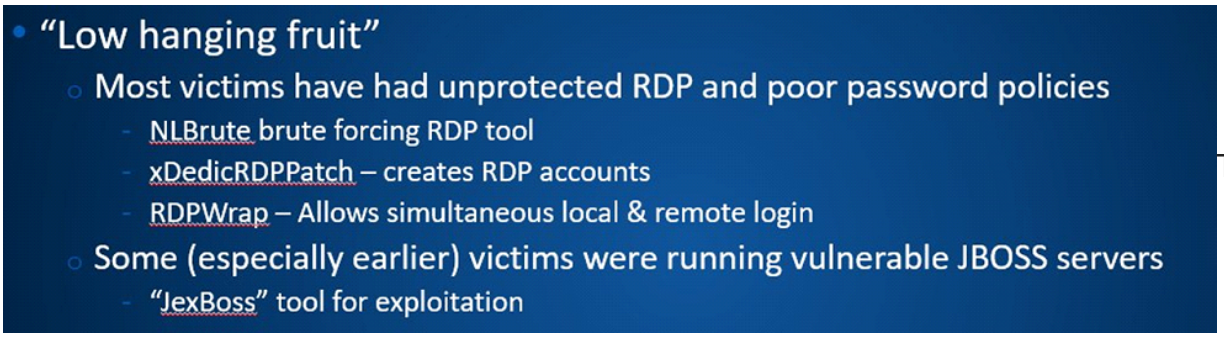
Summary of the attack procedures used by SamSam

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.



SamSam 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.

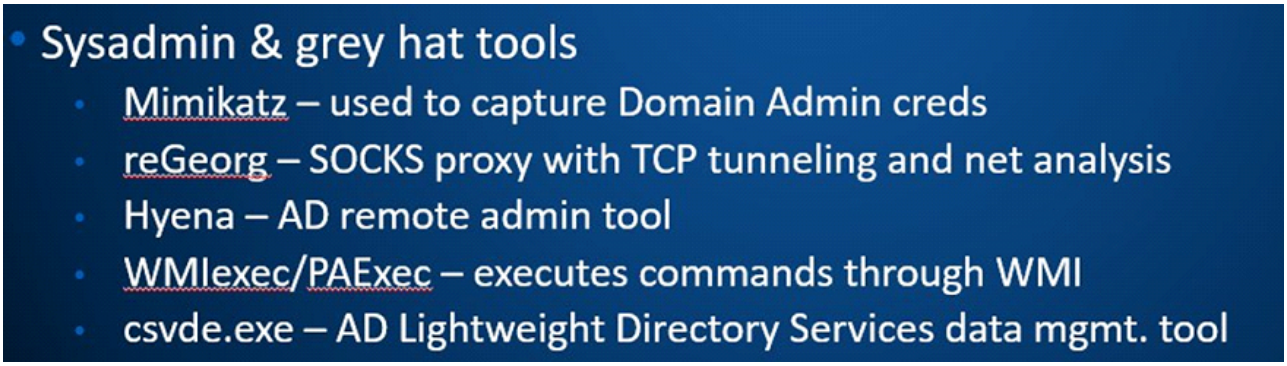


Tools employed by SamSam during the intrusion phase of the attack

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.

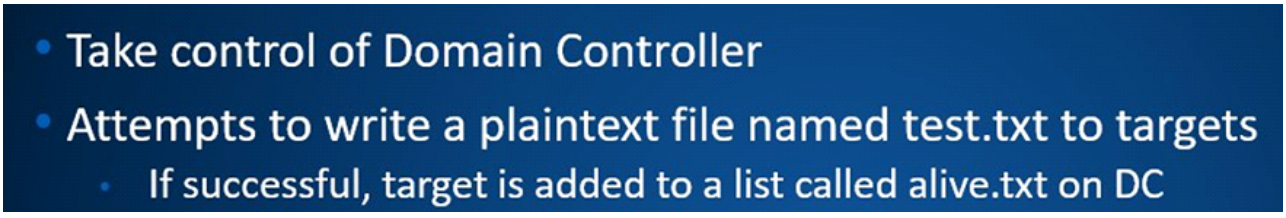
> If you have ports open in your firewall to let RDP through from the internet, and it isn't behind a VPN, **please close those ports now.** It doesn't matter how strong the Windows password is. It is **not worth the risk** to keep it open.

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.



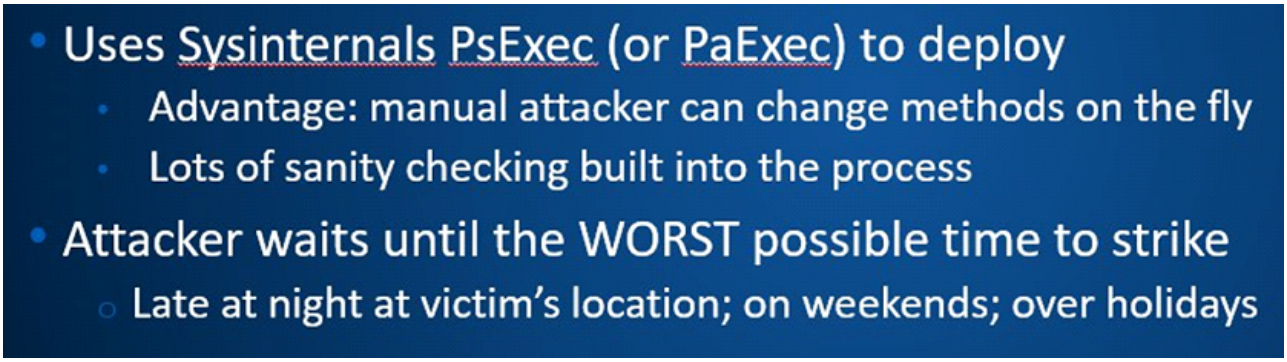
SamSam use conventional systems administration and some grey-hat hacking tools

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.



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.



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.

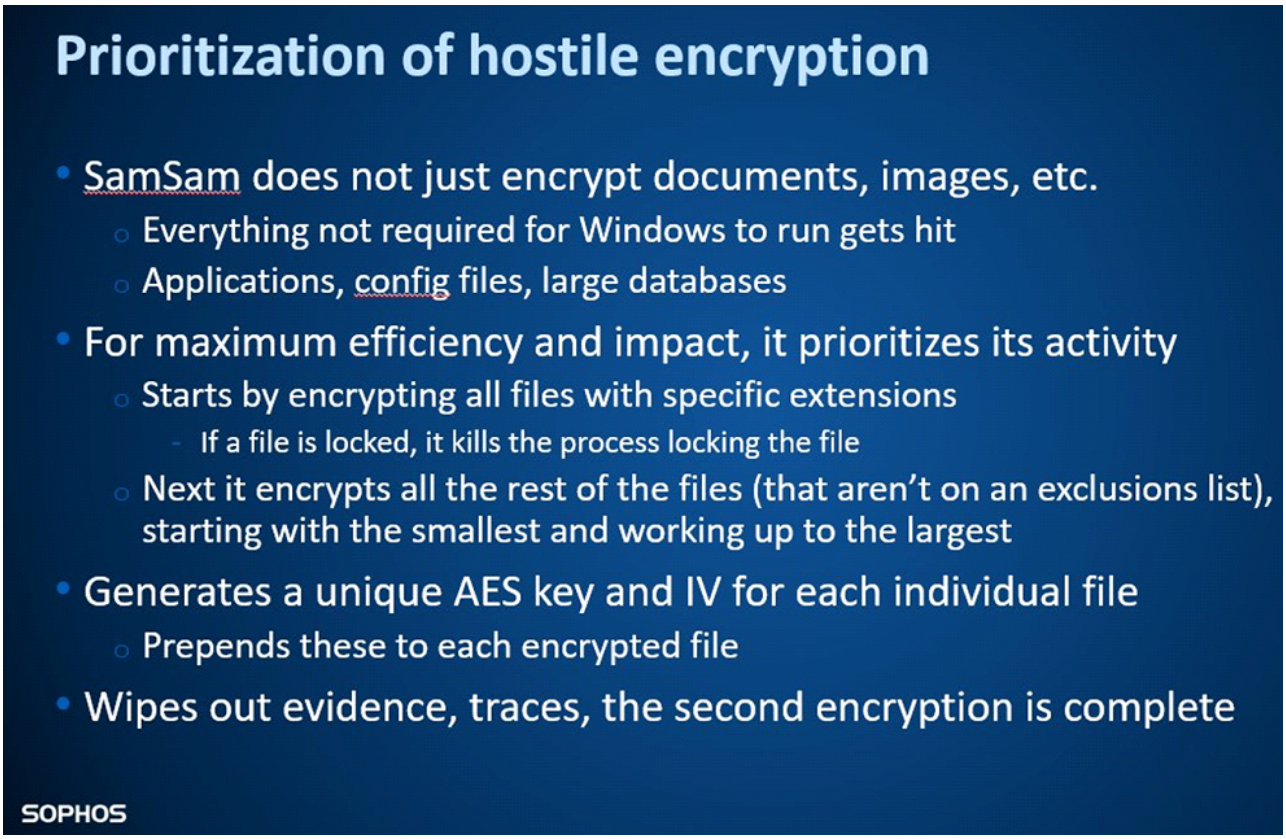
They waited until late at night, over weekends, or holidays to launch the attack, when the fewest people might notice before it was too late.

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 any 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.



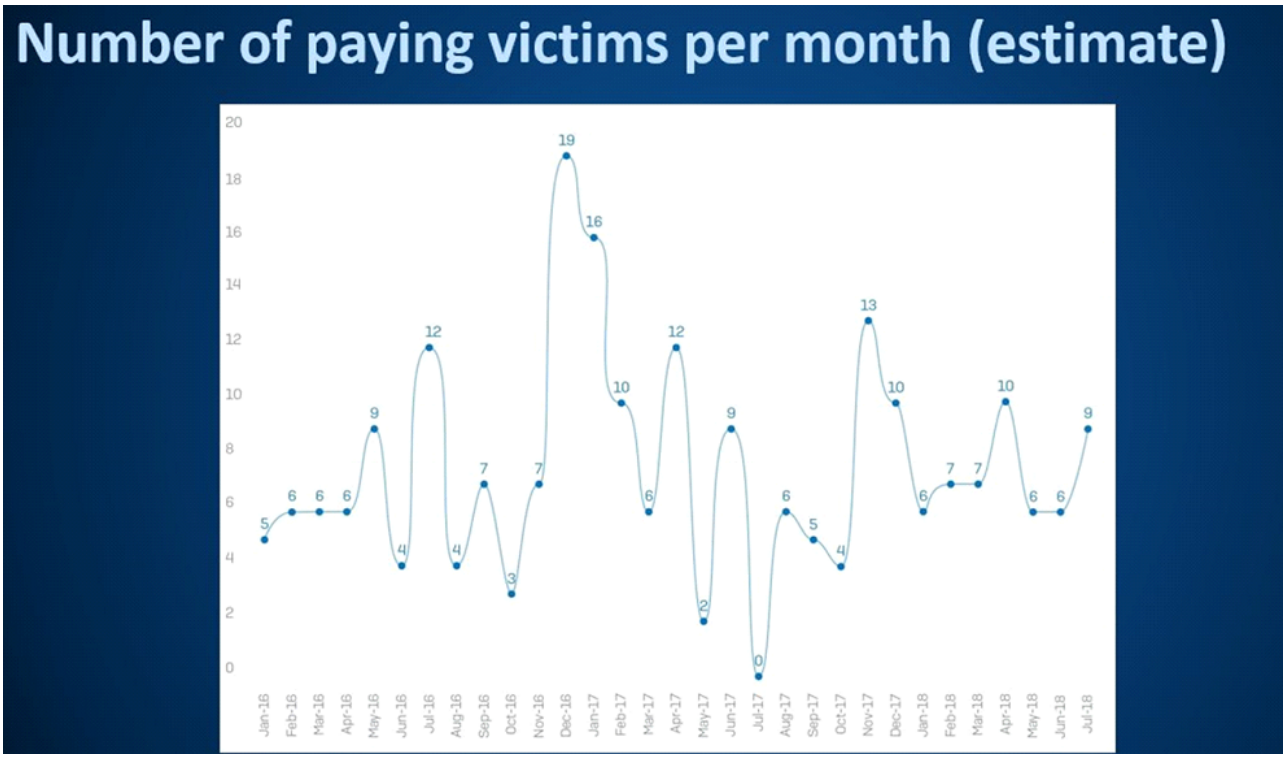
The SamSam attackers refined the encryption procedure many times over two years
The SamSam ransomware pushed the limits for efficiency, too. It encrypted the most important files first, and then *everything else* that wasn't essential to keeping the machine running.

The consquences 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?

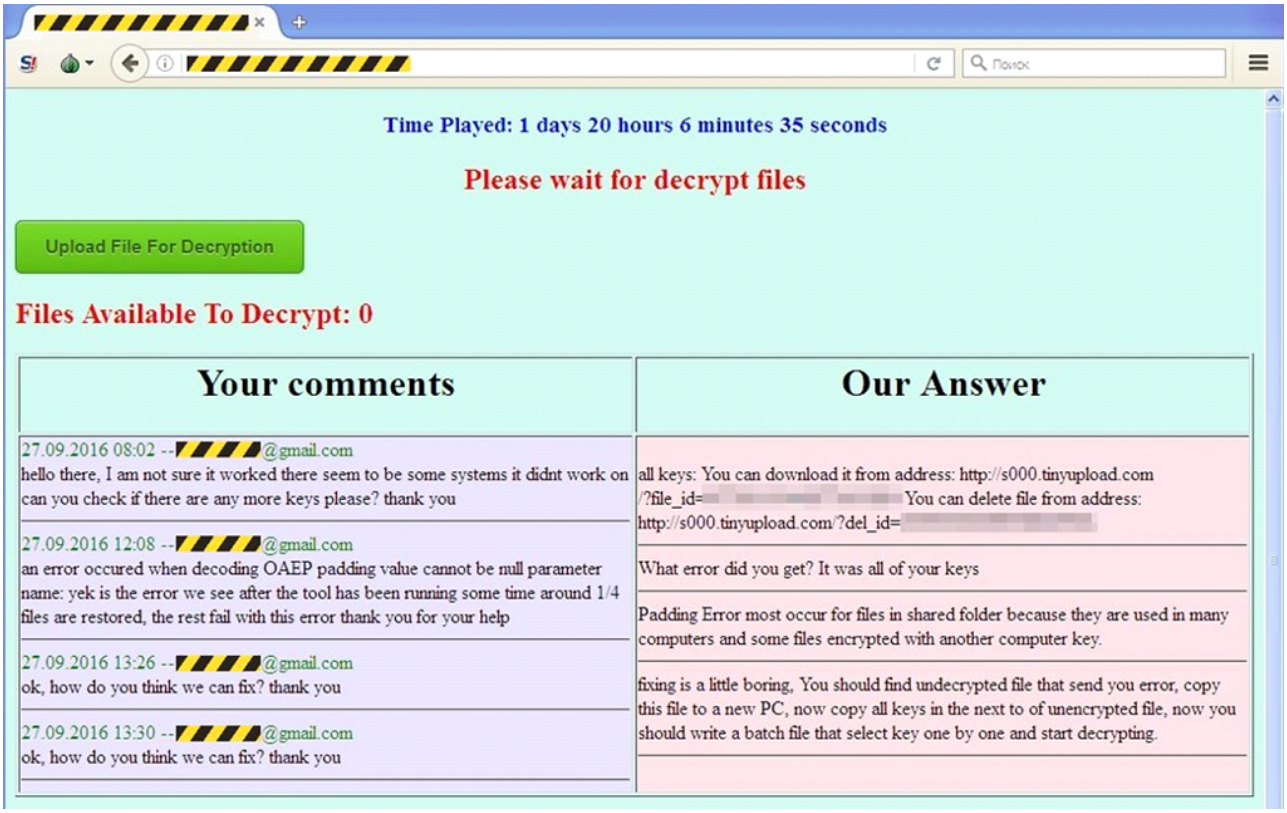
Could you do this for a massive global organization quickly enough not to incur heavy losses? What if you weren't just a gaming network and lives literally were hanging in the balance?

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.



SamSam only attacked a handful of organizations at a time, but had a high success rate

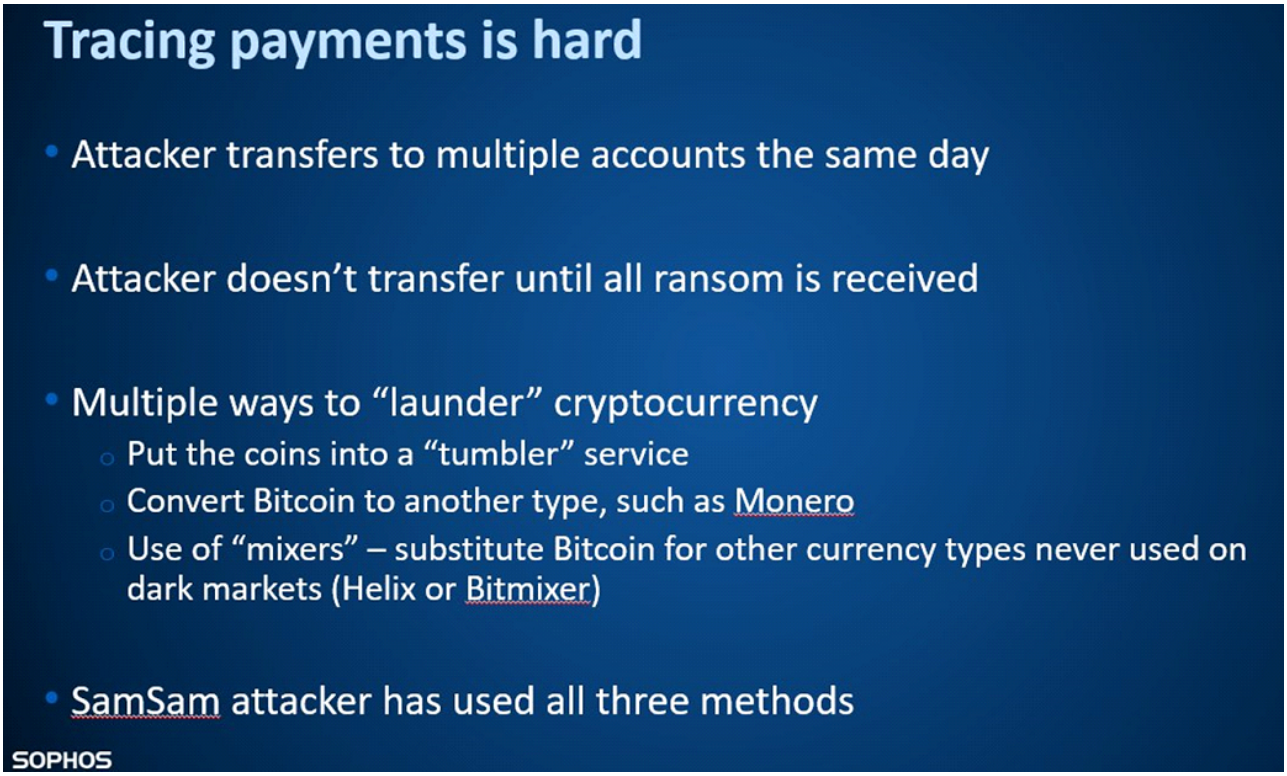
Every victim was provided with a unique .onion address on the dark web. At the other end, there was a kind of chat system where the victim interacted directly with the SamSam attackers.



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.



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.

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.

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