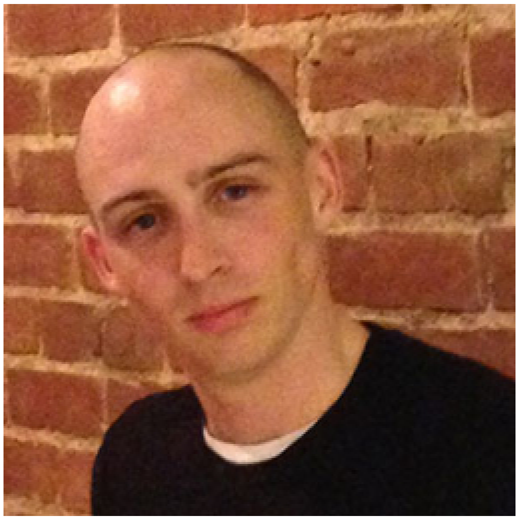
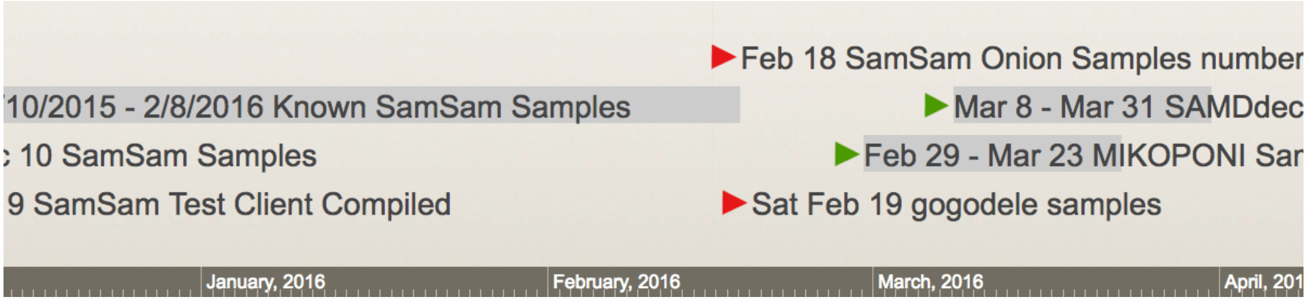
Targeted Ransomware Activity

anomali.com/blog/targeted-ransomware-activity

Research, Threat Intelligence Platform | April 14, 2016



by Aaron Shelmire



Overview

Since late 2013 there has been a growing trend of Ransomware activity. In these attacks actors encrypt files on hard drives, and request that a ransom be paid in order to decrypt the files. Many of these attacks have focused on client side vulnerabilities using phishing messages as a delivery vector. Since December 2015 there have been new ransomware intrusions that have been relying upon server side compromises. These compromises are used to deliver the SamSam ransomware family. As of the end of April 2016, the SamSam activity has targeted a minimum of 58 organizations including those in the HealthCare industry.

SamSam Activity

The samples related to the SamSam family are composed of 4 major samples. These are:

- SamSam - The name given to the original ransomware by the author

- MIKOPONI - A second major variation of SamSam. Much of the code base has evolved from SamSam, and the ransomware now directs users to a Tor site for payment.
- DelFileType - A tool used to delete files on the host. Original samples included the SysInternals sdel tool to delete the encrypted files from a host.
- SamDdec - The tool used to decrypt files after the ransom has been paid.

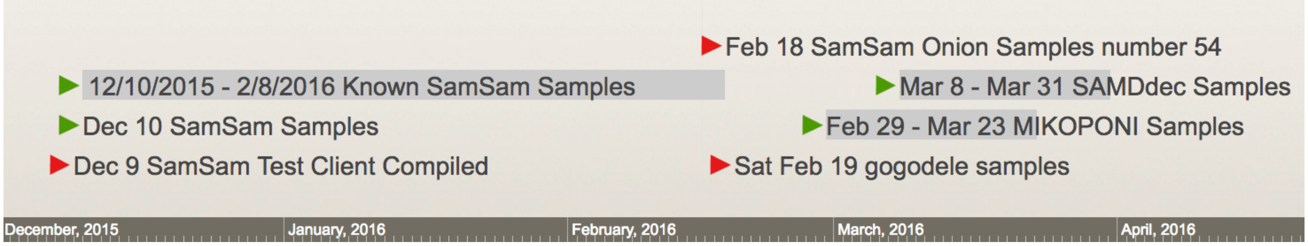
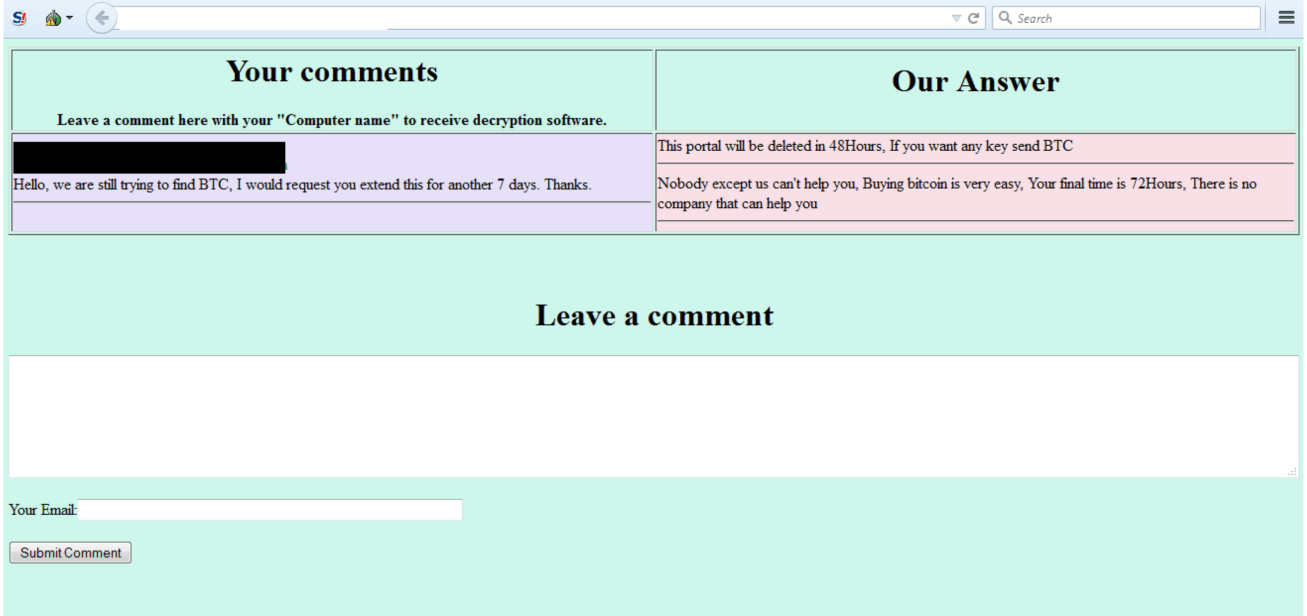


Figure 1: Timeline of SamSam Activity

The SamSam actors currently rely upon web pages on Tor hidden services for interacting with the victim organization. The actors ask that the victim pay the ransom using Bitcoin. The SamSam activity appears to have started around 9 December 2015 as is displayed in the Timeline in Figure 1. This is based upon the compilation time of a SamSam sample which includes a debug database path with “Test” in the path. The actor continued to label the PDB path for each sample with an incremental sample number until sample number 54, which has a compilation date of 18 February 2016. Up until this point the victims were sent to Wordpress sites for ransom instructions. The actor then began using Tor for the ransom sites, such as the one in Figure 2 below, as early as 23 February 2016. The actors began calling the ransomware MIKOPONI as early as 01 March 2016.



Your comments Leave a comment here with your "Computer name" to receive decryption software.	Our Answer
[redacted] Hello, we are still trying to find BTC, I would request you extend this for another 7 days. Thanks.	This portal will be deleted in 48Hours, If you want any key send BTC Nobody except us can't help you, Buying bitcoin is very easy, Your final time is 72Hours, There is no company that can help you

Leave a comment

Your Email:

Figure 2: SamSam Ransom Page

The SamSam actors appear to be storing the source code on a removable drive. This conclusion is based upon the PDB strings found within the compiled malware. Some examples of the PDB strings found within SamSam executables include:

```
d:SAMclientsSam41SAMobjReleasesamsam.pdb
f:SAMclients    estencSAMobjReleasesamsam.pdb
i:SAMServersSam-onion-no-check-lock-file-enc-all-extSAMobjReleaseMIKOPONI.pdb
l:SAMServersSam-onion - CopySAMobjReleaseMIKOPONI.pdb
u:SAMServersSam-onion-no-check-lock-file-enc-all-extSAMobjReleaseMIKOPONI.pdb
x:SAMServersSam-onionSAMobjReleaseMIKOPONI.pdb
```

These drive letters are atypical of standard Windows drive letter assignments. Usually the Windows operating system will assign the next available drive letter to a newly attached removable drive. If your computer only has a fixed drive with the C drive letter assigned, then the removable drive would be assigned the letter D. While the drive letter changes, the directory structure remains the same, which may be evidence of a removable drive. The drive letters D and F are more typical, but the other drive letters found in the PDB strings are odd.

The use of atypical drive letters could be caused by mounting an encrypted TrueCrypt container. In the TrueCrypt client the user is able to select a drive letter for mounting.

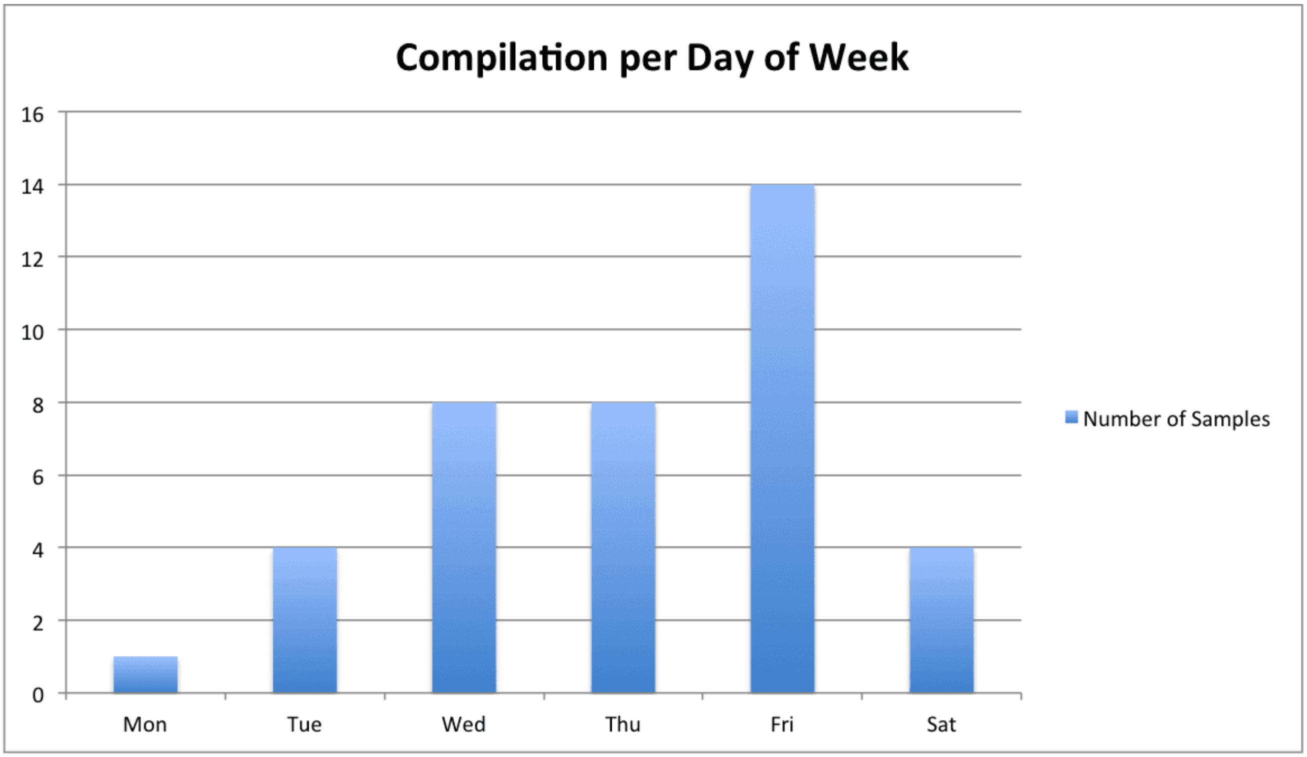


Figure 3: SamSam Day of Week Histogram

Based upon sample compilation times the SamSam actors appear to operate most frequently between 1700 and 0100 UTC, with samples compiled as early as 1000 UTC. If these compilation dates are accurate, this could mean that the actors are located in a Western nation, most likely within UTC+0200 to UTC-0400. The actors also appear to be most active within the work week on Fridays, with some activity on Saturdays.

Recent C0d0s0 / Peace Activity

The C0d0s0 a/k/a Peace actors have a long history of intrusion activity that has been related to them. This activity stretches back at least to October 2010 when the Nobel Peace Prize site was used to distribute their tools via a strategic web compromise leveraging a 0-day vulnerability in Firefox.

Since at least November 2015 the group has been utilizing JBOSS server vulnerabilities in order to gain access to target networks. This activity was described by Palo Alto Networks. Additional C0d0s0 activity is described by Proofpoint.

The C0d0s0 actors install a wide range of backdoors including PlugX, new variants of Derusbi, and Bergard. In at least one case, the C0d0s0 actors were operating on the same JBOSS server host where the SamSam tool was deployed. There have been some claims in the media that the SamSam activity is the work of the C0d0s0 group. At this point Anomali Labs has not been able to directly connect this activity. While both the SamSam activity and C0d0s0 activity have recently used JBOSS vulnerabilities, the different sets of activity appear to leverage different operating times. These times are almost complementary.

The presence of the two sets of tools on one host and the shared targeting of JBOSS could be coincidence. Evidence that shows a direct instance of a shared session of activity where actors interact with the C0d0s0 related artifacts AND SamSam related artifacts would contradict this. No such evidence has been presented.

Competing Hypothesis

There are a handful of additional hypothesis to explain a relationship between the C0d0s0 and SamSam activity.

The SamSam activity could be from a 2nd group that receives access to compromised hosts from the C0d0s0 actors after the C0d0s0 actors have gained a foothold.

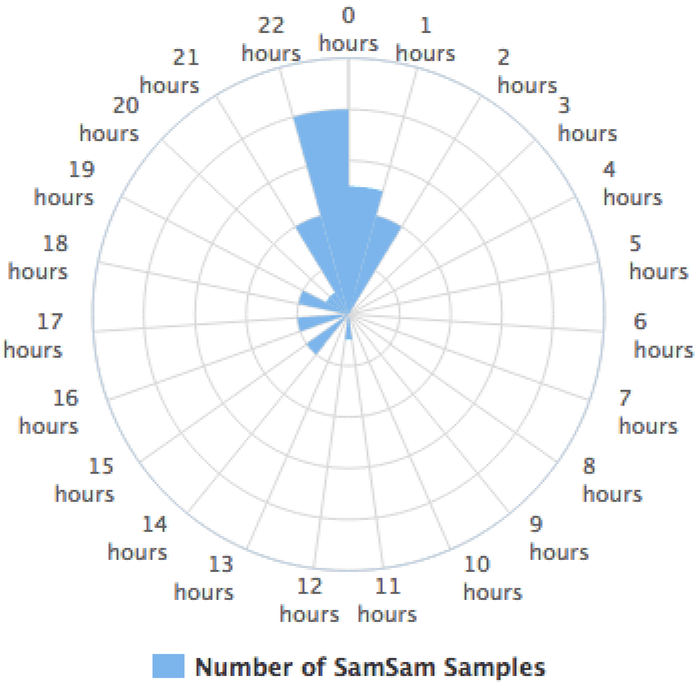


Figure 4: SamSam Compile Time Wheel

The SamSam activity could be activity from the C0d0s0 actors outside of their normal work duties. This theory is possible. The two sets of activity are nearly complimentary. The C0d0s0 activity mostly occurrs during 0300 - 1000 hours UTC, with less activity during 1200-1600 hours, and a few off hour samples. This activity is more easily aligned to time zones on the Asian continent, including China Standard Time (+0800).

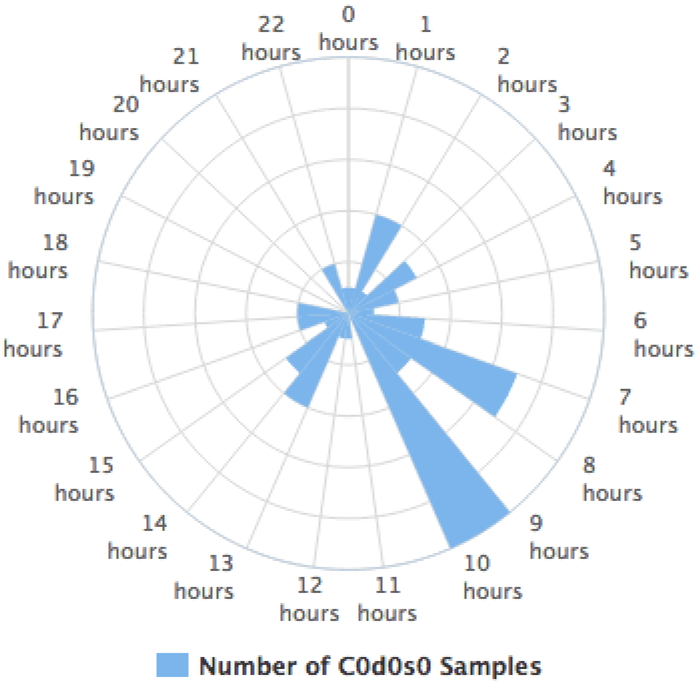


Figure 5: C0d0s0 Compile Time Wheel
The SamSam activity mostly occurs from 1500-0100 hours. There are two samples (out of 49) tied to the C0d0s0 group which fit the SamSam time profile. There are also 3 SamSam-related samples (out of 36) that fit the later portion of the C0d0s0 activity. If the SamSam activity is perpetrated by actors in China, they are operating in the middle of the night.

Key Assumptions Check

There are two key assumptions underpinning this analysis that put the conclusion at risk:

- We assume the compilation time of the samples has not been modified
- We assume the hosts that the samples have been compiled on have accurate Date/Time settings.

Another key assumption is that the C0d0s0 samples have been correctly attributed to one actor group. Similarly that the SamSam samples are correctly attributed to one actor group. We believe these two assumptions are less of a risk to the conclusions.

Finally, the C0d0s0 activity used as part of this analysis is absolutely a minor subset of the actors activity. It is possible that this sampling of activity is biased, and a full set of activity would result in different conclusions.

Free White Paper