SophosLabs releases SamSam ransomware report

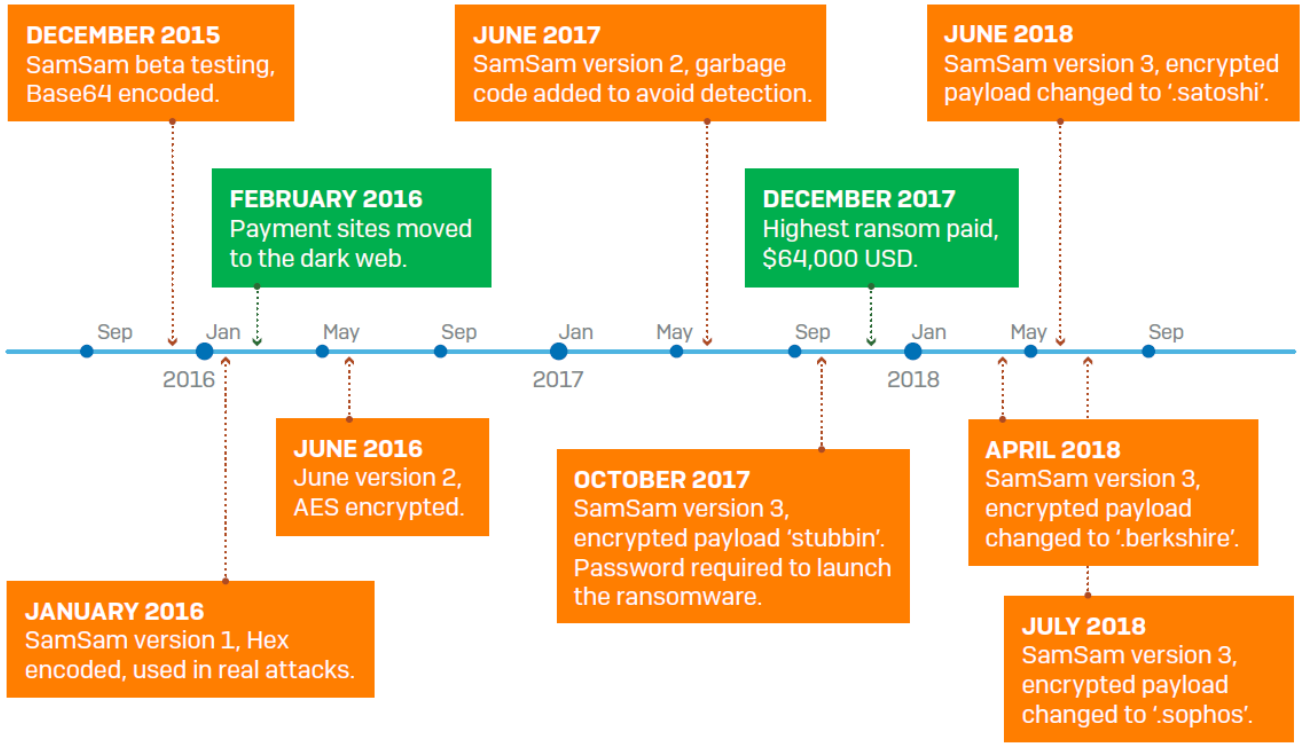
news.sophos.com/en-us/2018/07/31/sophoslabs-releases-samsam-ransomware-report/

Andrew Brandt July 31, 2018

By Andrew Brandt

It strikes in the dead of night, timing the moment when it begins to encrypt every hard drive it can reach to when the fewest IT administrators or SOC staff are likely to be on duty. Victims find few, if any, traces of the infection, other than a ransom note that demands payments exceeding $60,000 in Bitcoin, and links to a Dark Web customer support chat system that gives the victim an opportunity to trade text messages with the attacker.

SamSam's Evolutionary Timeline

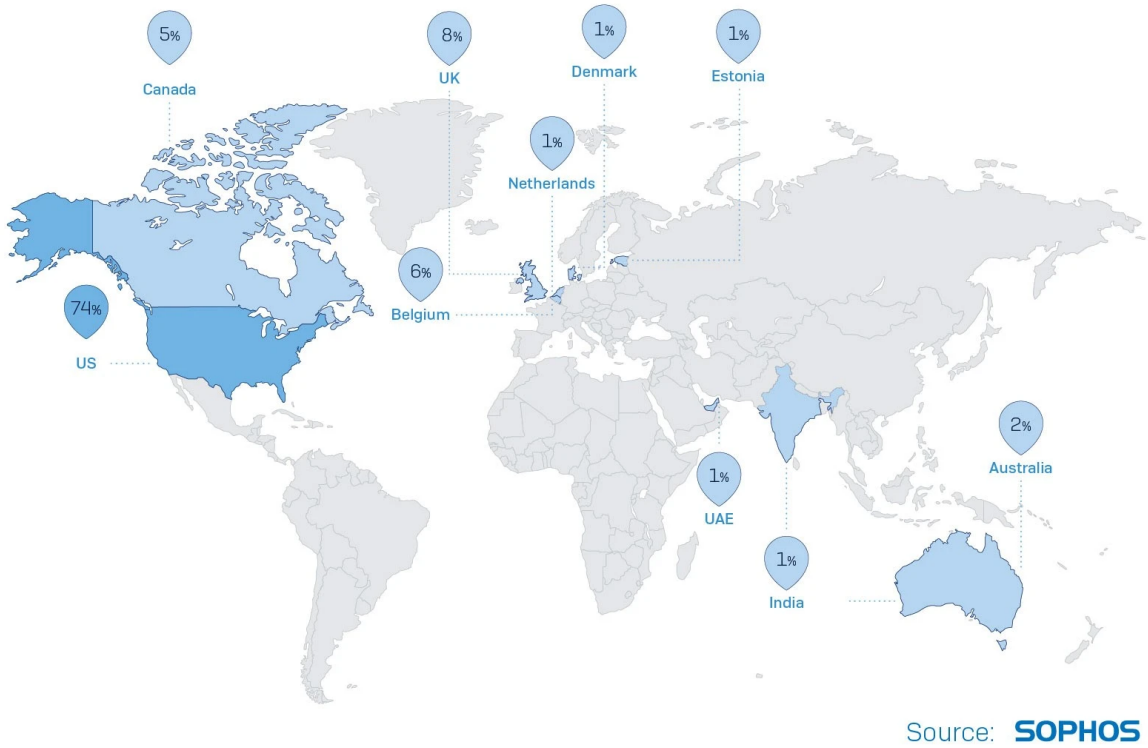


Source: SOPHOS

When *SamSam* appeared at the end of 2015, ransomware had really hit its stride, with a widely distributed variant of *CryptoWall* and new ransomware-as-a-service business models appearing. But this ransomware was different.

For one thing, SamSam's attack vector set it immediately apart from other ransomware. The person, or people, behind the attack employ a combination of old fashioned brute force attacks and exploits aimed at taking control of a single machine on the network of a targeted victim, before eventually taking control of a domain administrator machine. No malicious spam email or exploit kits delivered SamSam's payload. The attacker pushes it out to every workstation on a LAN domain and executes it simultaneously.

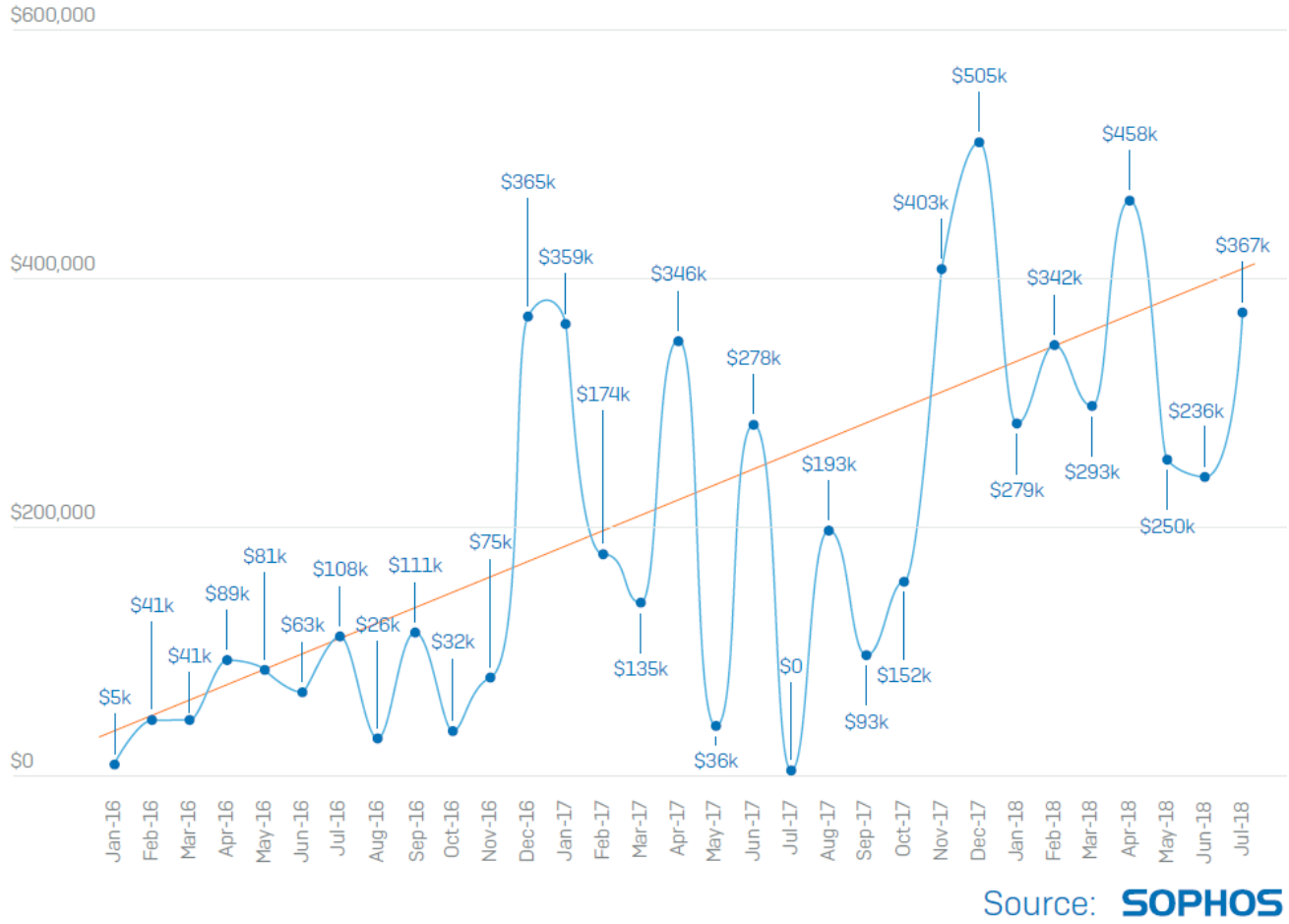
Percentage of SamSam victims by country, as identified by Sophos



For another, SamSam seems designed to maximize its own likelihood of success. A multi-tiered priority system ensures that the ransomware encrypts the most valuable data first, but eventually it also encrypts everything else that isn't in a very short list of Windows system-related files. Communication and payment involve Tor and Bitcoin for security and untraceability. The attacker personally launches the attacks using a combination of free, open source, and commercial network administrator tools.

The attacker actively evades security controls throughout the attack, deploying custom-compiled malware payloads and shutting down security measures as needed. It has been a particularly pernicious and heinous ransomware campaign, attacking hospitals, schools, municipal government, and even a homeless charity.

Many of the victims, by our analysis, have never publicly disclosed or acknowledged that an attack has even taken place, even though the Bitcoin transaction record irrefutably shows that a victim has paid the ransom, and each bitcoin address used by the SamSam attacker is unique to its victim organization.



The SamSam attacker has taken in **nearly $6 million** in ransom revenue since the malware appeared on the scene about 32 months ago, demanding a premium ransom in order to sell the victims a key that will decrypt every affected machine on the network. About one in four victims, according to our research, have paid the ransom rather than trying to recover from backups. We find out about new victims almost every week.

Our newly-released report, SamSam: The (Almost) Six Million Dollar Malware, is the result of more than six months' work by a team of SophosLabs malware analysts, reverse engineers, and Sophos senior support staff. These are just a few of the details that we cover in this in-depth analyis of both the malware and the tactics employed by this particularly challenged and paranoid threat actor.

We'll cover some of the side stories relating to the investigation in the coming days here on Uncut, but it's also worth mentioning: In the days leading up to the release of the report, the SamSam attacker has launched a new offensive targeting the reputation of Sophos itself. The latest version of the malware uses the file suffix .sophos on its encrypted payload.

Yeah, it’s a cute distraction, but it also says something important: We must be giving the right person or people a particularly hard time if they’re so irritated by us that they feel compelled to call us out by name. Giving bad guys a bad day makes me feel warm and fuzzy inside.