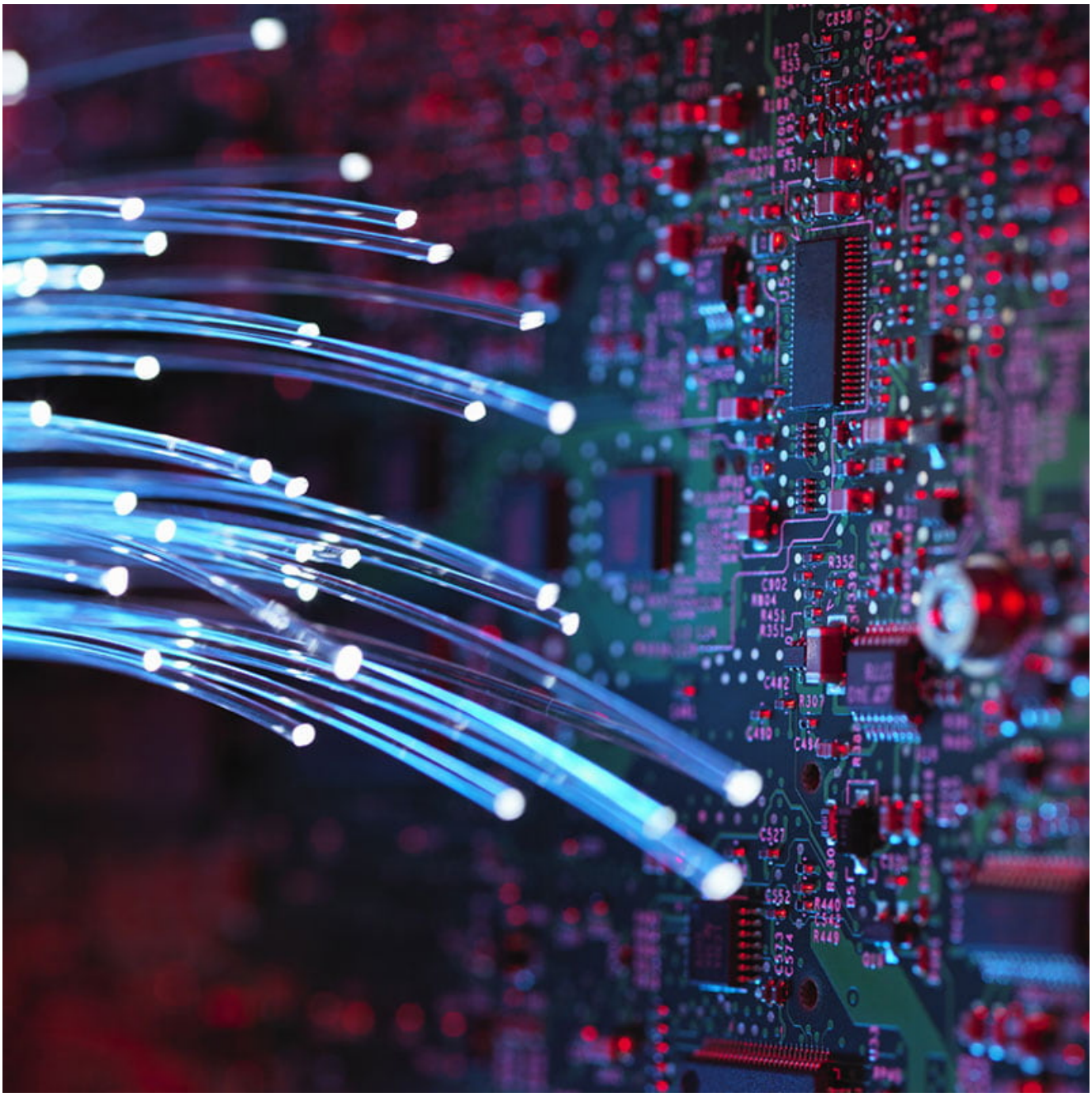
SamSam: Converting Opportunity into Profit

secureworks.com/blog/samsam-converting-opportunity-into-profit

Counter Threat Unit Research Team



Threat actors continue to use opportunistic attacks to compromise networks and deploy SamSam ransomware to collect money from various types of organizations.

Thursday, February 15, 2018 *By: Counter Threat Unit Research Team*

On February 15, 2018, Secureworks® Counter Threat Unit™ (CTU) researchers published details about the tools and techniques used in a series of high-profile ransomware campaigns conducted by threat actors that CTU™ researchers refer to as GOLD LOWELL.

The threat actors extort money from victims by infiltrating networks and using this access to deploy the SamSam ransomware. By analyzing multiple GOLD LOWELL ransomware incidents, CTU researchers and Secureworks incident response (IR) analysts have developed an extensive body of knowledge about the group's intent, tactics, and behaviors.

SamSam incidents in 2016 and 2018 led many people to conclude that GOLD LOWELL targets healthcare organizations. However, Secureworks' visibility into the group's activity reveals that it is opportunistic and is not limited to specific industries. Since late-2015, Secureworks IR analysts have observed GOLD LOWELL attacks impacting organizations in a wide range of industries; for example:

- IT software providers
- Waste management businesses
- Academic organizations
- Transportation networks
- Business services firms
- Leisure and entertainment businesses

The threat actors typically identify and exploit vulnerable Internet-connected systems and protocols such as Remote Desktop Protocol (RDP) to gain a foothold in a victim's network. They then use publicly available tools to steal high-value usernames and passwords, leverage custom scripts to survey the network, and deploy SamSam ransomware to as many systems as possible.

Supporting the claim that there is "no honor among thieves," the threat actors sometimes attempt to capitalize on a victim's willingness to pay the ransom by increasing the decryption cost after a victim submits the initial payment. GOLD LOWELL requests ransom fees in Bitcoin, and the rise in Bitcoin values translates to higher payments to decrypt impacted systems. For example, the cost to decrypt a single system in 2015 was $650 (USD), whereas by late-2017 the value increased to $9,700 per system. A GOLD LOWELL campaign that spanned late-2017 to early-2018 generated at least $350,000 in revenue for the threat actors. These campaigns will likely be a fixture of the threat landscape as long as they continue to be lucrative.