Cause & Effect: Sodinokibi Ransomware Analysis | Tetra Defense

By Marlene Jones

Published: 2020-05-05 · Archived: 2026-04-05 14:32:40 UTC

In the early morning hours in March of 2020, a high-value target company experienced a Sodinokibi ransomware incident that impacted the vast majority of their user's workstations. This particular ransomware attack had a unique twist — video screen captures recorded the event, revealing that the threat actors accessed a live feed throughout the attack, and enabled them to actively monitor their victim's response when the ransomware was triggered.

Sodinokibi Ransomware Minute-By-Minute Timeline

Here's a glimpse of how the attack unfolded:

6:01 AM	Surveillance video feed shows a customer call center environment with four rows of cubicles. Four angles of view are in the office area, and there are three employees present. Operations appear normal, with each employee actively engaged in work on their respective workstations, and two of the three are on phone calls. A message at the top of the screen reads, "Your computer is being controlled by 'Tech Support.'" The threat actor moves the mouse across the screen and hides this message.
6:09 AM	The video feed shows two of the three employees suddenly stand up from their desks and begin to pace the room excitedly while also talking to each other. They point at their screens and gesture to

	each other. The third employee's computer still appears to be functional. The other two employees walk over, and all three begin to huddle over the one working machine. One of the three makes a call on his cell phone and starts nervously pacing, even pulling his hair. A message at the top of the screen reads, "Your computer is being controlled by 'Tech Support.'" The threat actor scrolls the mouse across the screen and hides this message.
6:19 AM	One of the three employees walks out into the hallway, still on his phone. He is seen visibly wiping the sweat from his brow and his hands. He's gesturing and talking to someone on the phone as the other two employees continue to pace and try to work on the problem inside the call center. The employee walks back into the room from the hallway and sits, head in hands, pulling his hair. "Your computer is being controlled by 'Tech Support.'" The threat actor hides this message.
6:28 AM	All three employees are sitting around the call center, periodically making calls or texting, and now look defeated as well as distressed. One of the employees gets a phone call and suddenly stands up and runs out of the room and down the hallway. "Your computer is being controlled by 'Tech Support,'" hidden for the last time.

Our Forensic Analysis Team

Senior Director of DFIR Brad Roughan, Director of DFIR Bryan Mermilliod, and Director of DFIR Rahil Aftab teamed up to tackle this case. They confirmed the ransomware variant as Sodinokibi/REvil, and the root point of compromise to be from a cloud-based RMM (Remote Management and Monitoring) solution named "ConnectWise Control." This RMM tool allows for remote management and access to every computer within a network that has the software agent installed and registered within the tenant. In addition to remote access, ConnectWise also allows for the ability to patch, issue commands to remotely run programs, push scripts, create and schedule tasks, send messages, record sessions, and distribute files of any type. In ScreenConnect, when extended logging is enabled, all screenshare sessions are recorded, so anytime someone (authorized or not) remotes into a computer using the software, user activity is captured.

ScreenConnect is not a new target for Sodinokibi threat actors. Due to its administrative capabilities, Managed Service Providers, software providers, and companies that have public-facing and cloud-hosted implementations of ConnectWise are often specifically targeted. Unfortunately, when RMM tools such as ConnectWise are compromised, it allows a threat actor to quickly and effortlessly take over entire networks and to conduct malicious activities undetected and at their discretion. We have seen numerous cases where RMM tools are to mass-deploy ransomware to downstream customers of MSPs. Many of these cases have involved ConnectWise in conjunction with Sodinokibi.

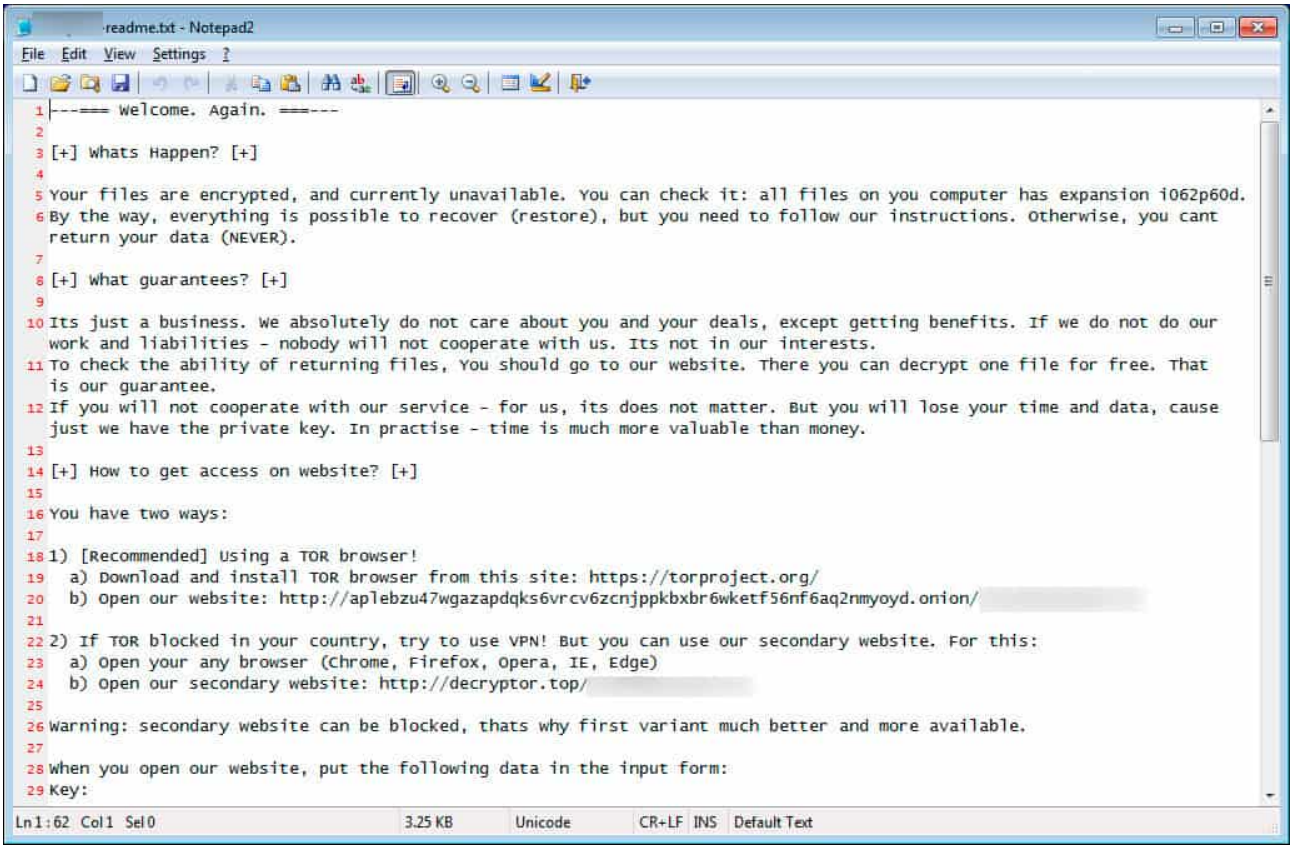
Tetra Defense performed forensic analysis on the client's systems during the investigation. Because extended logging was enabled in ConnectWise, we were able to review screen captures of the threat actor's activities on computers that they remoted into. Rahil Aftab commented, "It was really interesting to be able to compare the screen capture video to the underlying forensic artifacts. We saw how the threat actor's activities and the artifacts left behind compared to the videos from the affected systems."

How the Network was Compromised

ConnectWise transaction logs showed that on the day of the ransomware attack, connections for a user called "Tech Support" occurred from two IP Addresses: one out of Russia and one from New York. These IP addresses were not associated with any previous legitimate connections made from this user account.

When the Sodinokibi attack began, the "Tech Support" user issued a ConnectWise Control command to over 2,500 computer systems across the client's network. Its logs revealed that a base64 encoded Windows PowerShell script command was staged, submitted, and completed by the threat actor. Once the code was in place, a task named "RanCommand" was performed, effectively starting the Sodinokibi encryption process across the network.

The second stage of the script actually executed the Sodinokibi ransomware, encrypted targeted files on the system, and rendered them inaccessible. The script also removed Windows Volume Shadow Copies — this prevents restoring the device. Finally, a unique ransom note with instructions about how to pay the ransom and obtain the decryption program was created. An example of one Sodinokibi ransom note is below:



We collected and analyzed the ConnectWise Control logs from 12 months before the encryption event, as attacks of this nature usually go unnoticed for a while before deploying. Tetra was able to confirm that the "Tech Support" account, and all its administrative-level privileges, was compromised. This single user gave the threat actor full access to the network.

Sodinokibi Ransomware Meets Risky Business

This client, in particular, felt quite blindsided by this attack — they had enforced several precautions across the board and implemented some security best practices. They felt they had good systems to prevent Sodinokibi, so how could an attack like this happen to them?

While the high-value target company reported that two-factor authentication was enabled (and should have prevented a login from an unknown 3rd party), Tetra discovered that the employee behind the “Tech Support” user account never completed the process of setting up multifactor authentication. Other artifacts from the “Tech Support” user’s laptop showed numerous risky user behaviors prior to the attack. There was a saved text file containing user credentials and passwords — both to their desktop and to a personal online account. Personal cloud accounts were on their work laptop, and they were actively using torrents to search for, download, and install movies and cracked software. What’s most glaring is that the “Tech Support” user had sent email attachments including a username and password list — a spreadsheet containing employee names, phone extensions, and IP addresses, all in plain text.

“As we got further into the case, it evolved into a unique mix of both an investigation of an active ransomware attack and an internal investigation of missteps taken by an IT employee. It’s one of the more interesting cases I’ve seen recently,” said Brad Roughan. Bryan Mermilliod commented, “With both external and internal risks at play, the client was understandably on high alert throughout the restoration process. Our ability to detect malicious activity combined with our experience rebuilding and troubleshooting systems after these attacks allowed us to give the client peace of mind as they returned to ‘normal.’”

As unsettling as it is to be surveilled in a compromising situation, there is a silver lining to this case. Thankfully, as evidenced by extended logging in ConnectWise, there was no sign of data exfiltration. This threat actor was solely focused on compromise and encryption rather than stealing the client’s data.
