# Examining a Sodinokibi Attack

By By: Trend Micro Research Jan 26, 2021 Read time: 2 min (481 words)

Published: 2021-01-26 · Archived: 2026-04-05 20:22:33 UTC

Sodinokibi was first detected in April 2019 and linked to the retired GandCrab. From that point on, Sodinokibi launched several high-profile attacks that continued throughout 2020, thus making a name for itself as one of the ransomware families that should be watched out for. Here we describe Sodinokibi's typical attack process.

Technical analysis

The threat actors behind Sodinokibi typically hire a variety of affiliates for their initial access. Their attacks often begin with familiar techniques like malspam emails with spear-phishing links or attachments, RDP access that uses valid accounts, compromised websites, and exploits. They also use techniques that indicate their targeted approach.

***Initial access***

We observed the use of several of these initial access techniques. For example, as with campaigns, we saw the use of the CVE-2019-2725 vulnerability and observed an instance where Sodinokibi was loaded in the memory of PowerShell through reflective-load instead of binary execution. We also saw malspam that led to the use of a macro to download and execute the malware.

CVE-2018-13379 and CVE-2019-11510 are also used by the malware, as well as compromised valid accounts. This allows the threat actors to drop and execute other components like the anti-antivirus, exfiltration tools, and finally Sodinokibi itself.

***Lateral movement and evasion tactics***

Sodinokibi, like many ransomware families known today, have a targeted approach with regard to their campaigns. In line with this, we observed the use of RDP and PsExec for lateral movement — a sign of targeted attacks — to drop and execute other components and the ransomware itself.

We also observed that PC Hunter and Process Hacker are used to terminate services or processes, especially those services and processes that are related to antivirus software.

Once the system is infected, Sodinokibi sends a report and system information to its command-and-control (C&C) server. It generates a pseudorandom URL based on a fixed format and generation to add to a list of domains in its configuration.

Security recommendations

Sodinokibi has been known to target high-profile entities and uses notable evasive tactics. Organizations should, therefore, be wary of its techniques. For now, here are some best practices to prevent similar ransomware attacks:

- Avoid opening unverified emails or clicking on their embedded links, as these can start the ransomware installation process.
- Back up your important files using the 3-2-1 rule: Create three backup copies on two different file formats, with one of the backups in a separate location.
- Regularly update software, programs, and applications, to ensure that your apps are current, with the latest protections from new vulnerabilities.

If you believe that your organization has been affected by this campaign, visit this page for the available Trend Micro solutions that can help detect and mitigate any risks from this campaign.

Indicators of Compromise (IOCs)

| SHA256 | Detection name |
|---|---|
| 04ae146176632509ab5239d0ec8f2447d7223090 | Ransom.Win32.SODINOKIBI.MRA |
| 10682d08a18715a79ee23b58fdb6ee44c4e28c61 | Ransom.Win32.SODINOKIB.SMTH |
| 169abe89f4eab84275c88890460a655d647e5966 | Ransom.Win32.SODINOKIB.SMTH |
| 20d90f04dcc07e1faa09aa1550f343c9472f7ec6 | Ransom.Win32.SODINOKIB.SMTH |
| 2a75db73888c77e48b77b72d3efb33ab53ccb754 | Ransom.Win32.SODINOKIBI.AUWUJDES |
| 58d835c3d204d012ee5a4e3c05a06e60b4 316d0e | Ransom.Win32.SODINOKIB.SMTH |
| Ce0c8814d7630f8636ffd73f8408a36dc0e1ca4d | Ransom.Win32.SODINOKIB.SMTH |

---

Source: https://www.trendmicro.com/en_us/research/21/a/sodinokibi-ransomware.html