Sodinokibi: Aggressive Ransomware Impacting HPH Sector

Health Sector Cybersecurity Coordination Center (HC3)
HC3@HHS.GOV

Date: Sep 4, 2019

EXECUTIVE SUMMARY:

A relatively new ransomware named Sodinokibi is exploiting US-based organizations with successful attacks on dozens of Texas local municipalities and hundreds of dental practices. [i, ii, & iii] These most recent attacks are notable because they reportedly began with initial attacks on Managed Service Providers (MSPs) or Cloud Service Providers (CSPs) before spreading to many of the customers of those providers. This approach allows the Sodinokibi group to quickly increase the number of impacted organizations and their ransom demands through existing connections among organizations. Sodinokibi leverages a mixture of initial vectors for gaining a foothold within networks, and is thought to be related to the GandCrab ransomware family. Sodinokibi does not launch attacks within many former eastern-bloc nations or Syria. Protections from Sodinokibi are familiar defense-in-depth cyber protections, and include maintaining a regular and reliable backup (notably separate from host systems), updating operating systems and application software (including security software), and training users on how to respond to social engineering (e.g. phishing and unknown downloads).

The large number of impacted organizations and the targeting through service providers make it important for organizations within the Healthcare and Public Health (HPH) sector to maintain secure backups and up-to-date systems, while working with service providers' organizations to ensure the security of organizational data.

ANALYSIS:

Otherwise known as REvil, Sodinokibi is being associated with the recently "retired" GandCrab ransomware due to similarities in the program code and delivery methods. [iv & v] Some of the initial versions of Sodinokibi were also distributed alongside the GandCrab ransomware. Much like GandCrab, Sodinokibi is sold as Ransomware-as-a-Service[iv] meaning criminals are able to rent attack services to target the systems of their victims.

Infection & Distribution

Security researchers have identified several infection vectors used to distribute Sodinokibi including unpatched systems[vi,vii], hijacked websites[viii], and social engineering efforts targeting enterprise and consumer systems. In April 2019, Talos reported Sodinokibi leveraging vulnerable Oracle WebLogic enabled servers (CVE-2019-2725) to download and distribute the malware.[vii] In June, a web page belonging to an Italian distributor of WinRaR software was altered to distribute Sodinokibi.[ix] In other cases, Sodinokibi was distributed via an embedded macro in a Microsoft Word document, or via a compressed JavaScript file or executable.[x]

Sodinokibi Ransomware Operation

Once a foothold is established, the malware seeks to gain elevated system privileges or attempt to bypass Windows' User Access Control.[iii] Some instances of Sodinokibi have searched for antivirus created by the South Korean security vendor Ahnlabin order to disable and hijack the security application's own processes.[iii] However, even without this application, Sodinokibi will use PowerShell to execute its payload. The malware will then target Windows vulnerability (CVE-2018-8453) to gain administrator access, communicate with Command and Control servers (C2) for download, check the nationality of the targeted computer (i.e. CIS countries), and will then proceed to run. The ransomware will then delete shadow file copies and will use PowerShell and Remote Desktop Software (Webroot Management Console, or if it is disabled, ConnectWise Control/ScreenConnect) to distribute malware to connected systems.[i & iii] Finally, many common user content file types are encrypted, a ransom note is provided in each folder containing encrypted files, the system's wallpaper/background is changed, and the user is prompted with a web page containing the ransom note.[iii] Ransoms have been reported at $5,000 per client and, with hundreds impacted, have exceeded $200,000[ix].

PATCHES, MITIGATIONS, & WORKAROUNDS

Consumer recommendations[v]

1. Back up all files and systems. Keep these backups secure:
    a. Isolate backups from their host systems and network
    b. Ensure that you can recover the files if needed
2. Update your systems with the latest patches
    a. Operating Systems (including mobile devices)
    b. Application Software
    c. Security Software (Antivirus and antimalware)
3. Disable macros on Microsoft Office Products
4. Use effective cybersecurity hygiene to avoid social engineering attempts, such as
    a. Phishing – avoid opening files from entities whom you aren't expecting an attachment
    b. Pharming – avoid downloading and opening unknown/uncertified files from the Internet

Enterprise Infrastructure recommendations[v]

In addition to the above recommendations, enterprise administrators are suggested to implement the following.

1. Disable Remote Desktop Protocol and/or deny public IP access to RDP port 3389
2. Block unused ports and disable unused network services
3. Apply attachment filtering to email messages

4. Ensure that users are trained to recognize social engineering, and how to handle suspicious email and downloads.

Indicators of Compromise (IoC) – please see referenced material or contact HC3 for more information.

Vulnerabilities noted

- CVE-2018-8453 – "Win32k Elevation of Privilege Vulnerability" (CVE Base Score 7.8 **High**) affecting Windows 7, 8.1, and 10, and Windows Server 2008, 2008 R2, 2012, 2016, and 2019
    - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8453
    - https://nvd.nist.gov/vuln/detail/CVE-2018-8453
- CVE-2019-2725 "Oracle Security Alert Advisory" (CVE Base Score 9.8 **Critical**) affecting Oracle WebLogic Servers;
    - https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html
    - https://nvd.nist.gov/vuln/detail/CVE-2019-2725

---

[i] Fernandez, M. Sanger, D. & Martinez, M., "Ransomware Attacks Are Testing Resolve of Cities Across America", 22 Aug 2019, accessed 3 Sep 2019; https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html

[ii] Ilascu, I., "Sodinokibi Ransomware Encrypts Records of Hundreds of Dental Practices", 29 Aug 2019, accessed 3 Sep 2019; https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-encrypts-records-of-hundreds-of-dental-practices/

[iii] Krebsonsecurity.com, "Ransomware Bites Dental Data Backup Firm", 19 Aug 2910, accessed 3 Sep 2019; https://krebsonsecurity.com/2019/08/ransomware-bites-dental-data-backup-firm/

[iv] Krebsonsecurity.com, "Is 'REvil' the New GandCrab Ransomware?", 19 Jul 2019, accessed 3 Sep 2019; https://krebsonsecurity.com/2019/07/is-revil-the-new-gandcrab-ransomware/

[v] Van den Hurk, F., "A connection between the Sodinokibi and GandCrab ransomware families?", accessed 3 Sep 2019; https://www.tesorion.nl/aconnection-between-the-sodinokibi-and-gandcrab-ransomware-families/

[vi] Umawing, J., "Threat Spotlight: Sodinokibi ransomware attempts to fill GandCrab void", 18 Jul 2019, accessed 3 Sep 2019; https://blog.malwarebytes.com/threat-spotlight/2019/07/threat-spotlight-sodinokibi-ransomware-attempts-to-fill-gandcrab-void/

[vii] Cadieux, P. Grady, C. Schultz, J. & Valites, M. "Sodinokibi ransomware exploits WebLogic Server vulnerability", 30 Apr 2019, accessed 3 Sep 2019; https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html

[viii] Abrams, L., "Sodinokibi Ransomware Spreads via Fake Forums on Hacked Sites", 2 Sep 2019, accessed 3 Sep 2019; https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-spreads-via-fake-forums-on-hacked-sites/

[ix] Iiascu, I., "A Look Inside the Highly Profitable Sodinokibi Ransomware Business", 30 Aug 2019, accessed 3 Sep 2019; https://www.bleepingcomputer.com/news/security/a-look-inside-the-highly-profitable-sodinokibi-ransomware-business/

[x] Abrams, L., "Sodinokibi Ransomware Spreads Wide via Hacked MSPs, Sites, and Spam", 21 Jun 2019, accessed 3 Sep 2019; https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-spreads-wide-via-hacked-msps-sites-and-spam/