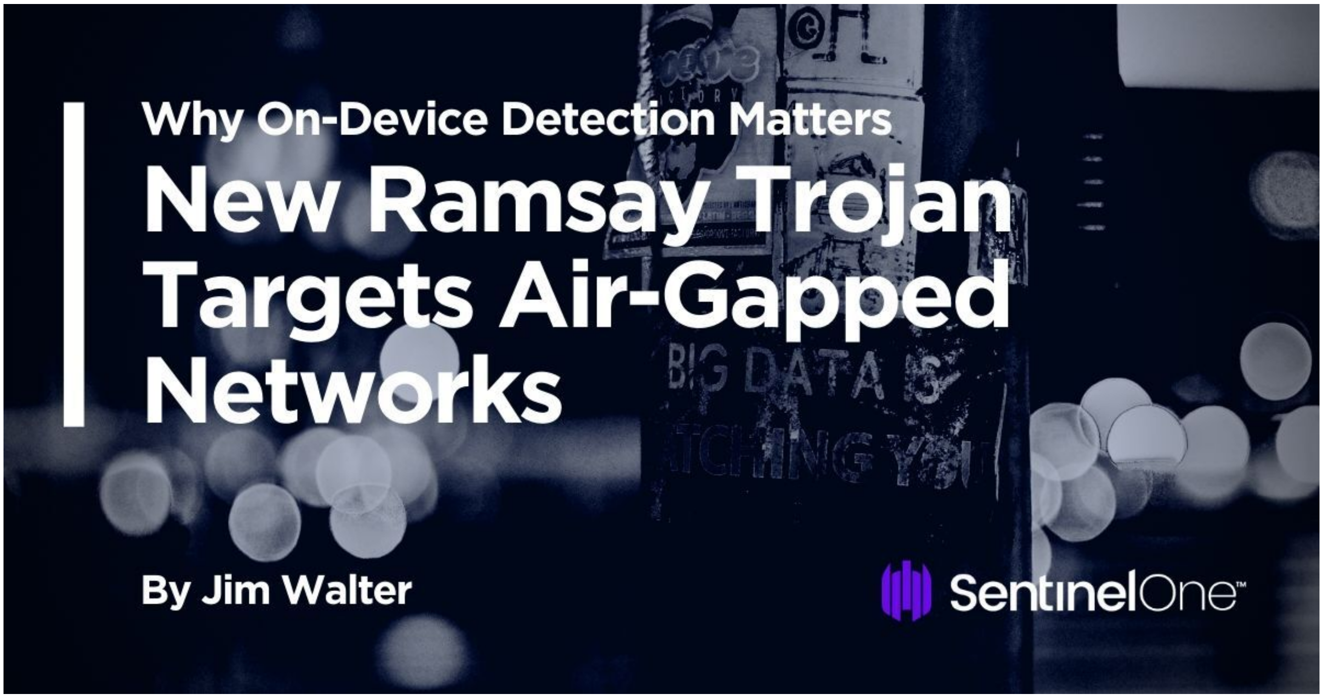
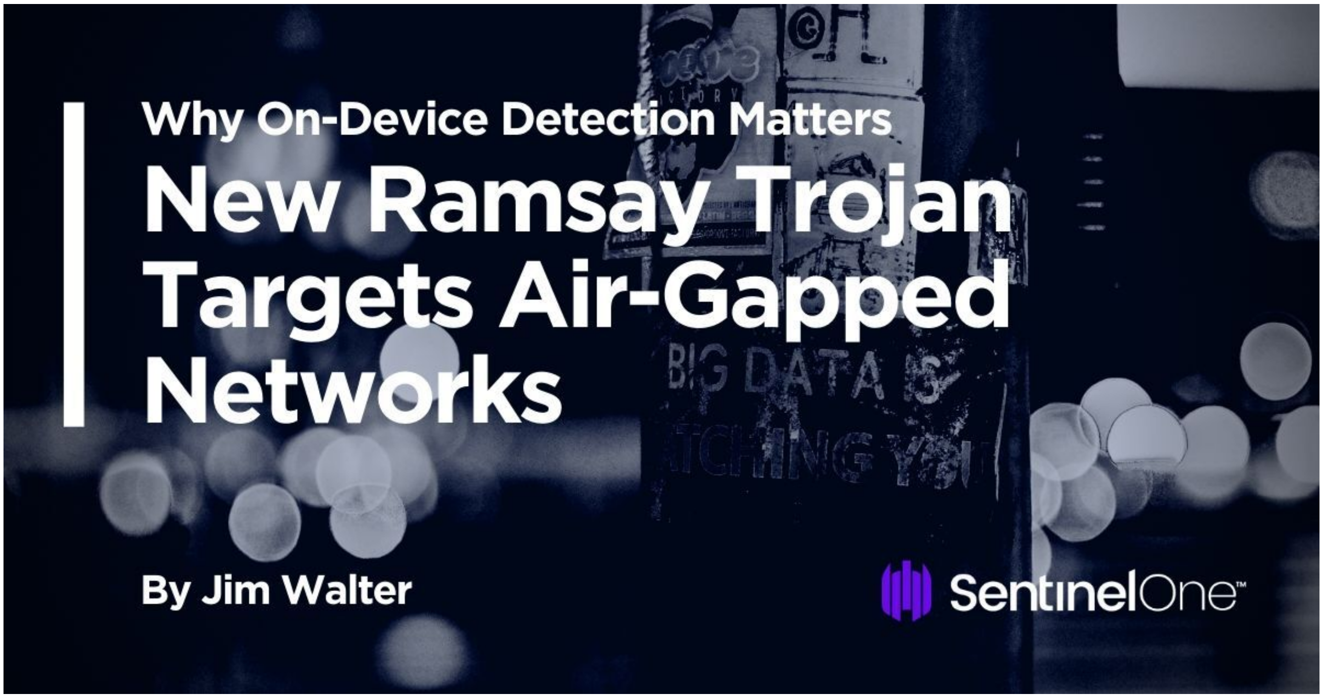
Why On-Device Detection Matters: New Ramsay Trojan Targets Air-Gapped Networks

sentinelone.com/blog/why-on-device-detection-matters-new-ramsay-trojan-targets-air-gapped-networks/

May 20, 2020


Why On-Device Detection Matters
New Ramsay Trojan Targets Air-Gapped Networks
By Jim Walter
SentinelOne

The Ramsay “framework” emerged in late 2019 and was disclosed thanks to a discovery by researchers querying the VirusTotal public malware repository. As of April 2020, there appears to be two fully maintained branches of the toolkit. Although in-the-wild instances of the Ramsay malware appear to be low at present, this may be due to the malware’s highly-specialized objectives. The Ramsay samples discovered to date are heavily focused on both persistence and data exfiltration from air-gapped environments. This suggests the possibility that the malware was developed for advanced targeted campaigns by a threat actor primarily interested in organizations trying to protect the most-sensitive of information. As is often the case with specialized malware, there is also a real danger of it “leaking” or being repurposed to targets that were not in the original threat actors’ sights.


Why On-Device Detection Matters
New Ramsay Trojan Targets Air-Gapped Networks
By Jim Walter
SentinelOne

Ramsay Distribution and Persistence

The original version of Ramsay was distributed via maliciously-crafted Office documents. These documents were distributed via email and were designed to exploit CVE-2017-0199 to facilitate the installation of the malware. CVE-2017-0199 is a remote code execution flaw in Microsoft Word. Specifically, it allows attackers to retrieve and launch code, including VBS & PowerShell, upon launching of a specially-crafted RTF document. Several versions of these malicious Word documents were discovered on VirusTotal with names such as “access_test.docx” and “Test.docx”, indicating that the threat actors may have been evaluating how well their malware fared against vendors’ static engines.

Later versions of Ramsay (v2.a/2.b) were distributed as trojanized installers for well-known applications such as 7zip. These later versions also included an aggressive spreading mechanism that locates local and network adjacent PE files and infect them to allow for further spreading in targeted environments.

Version 2.b was also seen to be exploiting CVE-2017-11882. This vulnerability allows attackers to achieve arbitrary code execution as the current user in a MS Office 2016 and several earlier Office Service Pack versions. Both CVE-2017-0199 and CVE-20170-11882 are used for exploitation of client execution (MITRE T1203) purposes.

Along with the spreading capabilities, Ramsay includes multiple techniques for maintaining persistence. These include:

- AppInitDLL Registry Key Entries
- Scheduled Tasks
- DLL Hijacking

While early versions used well-known persistence techniques such as loading custom DLLs into other application processes' address space and task scheduling, later versions leverage DLL Hijacking, specifically targeting msfte.dll and oci.dll dependencies of the Microsoft Search Service and the Microsoft Distributed Transaction Coordinator service, respectively.

Ramsay Observed Behavior

Ramsay's main goal is data collection and exfiltration. Immediately upon infection, the trojan will begin to locate specific document types, particularly MS Word and PDF format files, and store them in a customized location. The items are also archived and encrypted via RC4, and subsequently compressed with an instance of WinRar installed by the trojan. It should be noted that Ramsay will attempt to collect documents from both local and remote locations where possible. Ramsay also has some built-in "intelligence" to avoid the collection of duplicate/redundant files.

The analysis is ongoing with respect to the data exfiltration mechanism. Current intelligence indicates that an additional component will locate the collected "containers" of documents from infected hosts, identified by special file makers, When the containers are located, AND a Ramsay control file is located on the affected network, data exfiltration can occur via this additional component. Ramsay uses intra-network control files to operate, as opposed to a central command-and-control infrastructure.

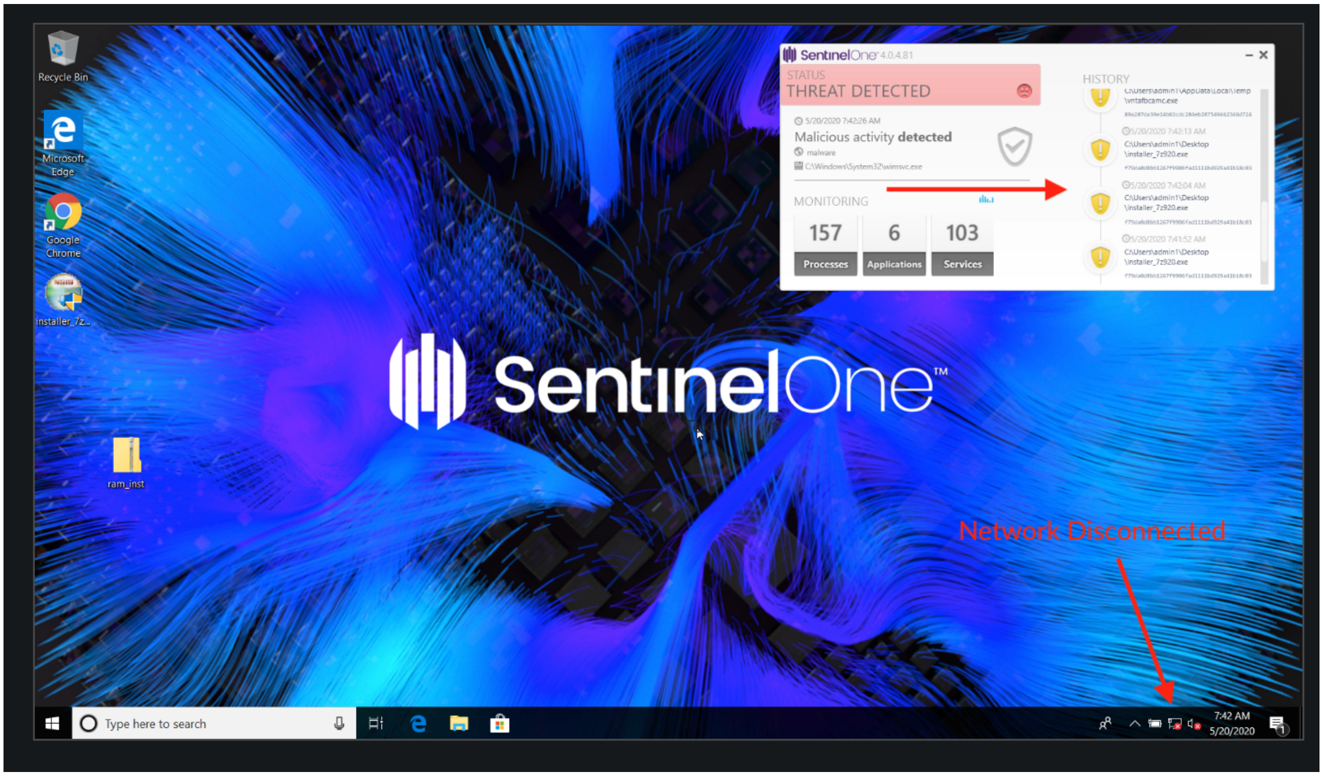
Spreading is handled via an additional component, dropped by the main installer. This component will scan and locate accessible drives/locations (excluding A: and B: reserved devices).

Given some level of code reuse, there may be correlation between Ramsay and the Retro Backdoor associated with Darkhotel. As with the data exfiltration piece, analysis of this relationship is ongoing.

Does SentinelOne Protect Against Ramsay Malware?

Yes, it does. Organizations secured by the SentinelOne platform are fully protected against the threat from Ramsay malware, as demonstrated in this video.

Even when the network is disconnected such as with an air-gapped device, the SentinelOne agent will detect the malware locally on-device.



SentinelOne 4.0.4.81

STATUS
THREAT DETECTED

5/20/2020 7:42:26 AM
Malicious activity **detected**
malware
C:\Windows\System32\wimsvc.exe

MONITORING

157	6	103
Processes	Applications	Services

HISTORY

C:\Users\admin1\AppData\Local\Temp\vntafbcamc.exe
89a287da39e14b02cdc28deb2875d9662346d724

5/20/2020 7:42:13 AM
C:\Users\admin1\Desktop\installer_7z920.exe
f79da0d8bb1267f9906fad1111bd929a41b18c03

5/20/2020 7:42:04 AM
C:\Users\admin1\Desktop\installer_7z920.exe
f79da0d8bb1267f9906fad1111bd929a41b18c03

5/20/2020 7:41:52 AM
C:\Users\admin1\Desktop\installer_7z920.exe
f79da0d8bb1267f9906fad1111bd929a41b18c03

Conclusion

The Ramsay framework is a novel malware toolkit that appears to be under active development by a sophisticated threat actor. While current telemetry suggests this is a highly-targeted attack focused on specific environments, history suggests that a malware toolkit of this nature could soon 'spread its wings' and represent a threat to a much wider audience. Moreover, the discovery of this new toolkit targetting air-gapped machines highlights the importance of having a behavioral, AI-driven security solution that can actively detect and respond to threats on the local device without solely relying on cloud-connectivity, human analysts or static reputation engines.

If you are not already protected by SentinelOne and would like to learn more about how our industry-leading platform can help defend your organization against Ramsay malware and all other threats, contact us or request a free demo today.

Sample Hashes for Ramsay Malware

SHA1: f79da0d8bb1267f9906fad1111bd929a41b18c03
SHA256: e60c79a783d44f065df7fd238949c7ee86bdb11c82ed929e72fc470e4c7dae97

SHA1: 3849e01bff610d155a3153c897bb662f5527c04c
SHA256: 22b2de8ec5162b23726e63ef9170d34f4f04190a16899d1e52f8782b27e62f24

SHA1: bd97b31998e9d673661ea5697fe436efe026cba1
SHA256: aceb4704e5ab471130e08f7a9493ae63d3963074e7586792e6125deb51e40976

SHA1: e7987627200d542bb30d6f2386997f668b8a928c
SHA256: 610f62dd352f88a77a9af56df7105e62e7f712fc315542fcac3678eb9bbcfcc6

SHA1: ae722a90098d1c95829480e056ef8fd4a98eedd7
SHA256: 823e21ffecc10c57a31f63d55d0b93d4b6db150a087a92b8d0e1cb5a38fb3a5f

SHA1: 19bf019fc0bf44828378f008332430a080871274
SHA256: 823e21ffecc10c57a31f63d55d0b93d4b6db150a087a92b8d0e1cb5a38fb3a5f

SHA1: 5c482bb8623329d4764492ff78b4fbc673b2ef23
SHA256: cc7ac31689a392a2396f4f67d3621e65378604b16a2420ffc0af1e4b969c6689

SHA1: bd8d0143ec75ef4c369f341c2786facbd9f73256
SHA256: dede24bf27fc34403c03661938f21d2a14bc50f11297d415f6e86f297c3c3504

SHA1: 5a5738e2ec8af9f5400952be923e55a5780a8c55
SHA256: 6f9cae7f18f0ee84e7b21995a597b834a7133277637b696ba5b8eea1d4ad7af1