Ramsay, Software S0458 | MITRE ATT&CK®

Archived: 2026-04-05 16:33:00 UTC

Enterprise T1548 .002 Abuse Elevation Control Mechanism: Bypass User Account Control

Ramsay can use UACMe for privilege escalation.[1][2]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Ramsay has used HTTP for C2.[2]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

Ramsay can compress and archive collected files using WinRAR.[1][2]

.003 Archive Collected Data: Archive via Custom Method

Ramsay can store collected documents in a custom container after encrypting and compressing them using RC4 and WinRAR.[1]

Enterprise T1119 Automated Collection

Ramsay can conduct an initial scan for Microsoft Word documents on the local system, removable media, and connected network drives, before tagging and collecting them. It can continue tagging documents to collect with follow up scans.[1]

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Ramsay has created Registry Run keys to establish persistence.[2]

Enterprise T1059 .005 Command and Scripting Interpreter: Visual Basic

Ramsay has included embedded Visual Basic scripts in malicious documents.[1][2]

Enterprise T1132 .001 Data Encoding: Standard Encoding

Ramsay has used base64 to encode its C2 traffic.[2]

Enterprise T1005 Data from Local System

Ramsay can collect Microsoft Word documents from the target's file system, as well as `.txt`, `.doc`, and `.xls` files from the Internet Explorer cache.[1][2]

Enterprise T1039 Data from Network Shared Drive

Ramsay can collect data from network drives and stage it for exfiltration.[1]

Enterprise T1025 Data from Removable Media

Ramsay can collect data from removable media and stage it for exfiltration.[1]

Enterprise T1074 .001 Data Staged: Local Data Staging

Ramsay can stage data prior to exfiltration in `%APPDATA%\Microsoft\UserSetting` and `%APPDATA%\Microsoft\UserSetting\MediaCache`.[1][2]

Enterprise T1140 Deobfuscate/Decode Files or Information

Ramsay can extract its agent from the body of a malicious document.[1]

Enterprise T1546 .010 Event Triggered Execution: AppInit DLLs

Ramsay can insert itself into the address space of other applications using the AppInit DLL Registry key.[1]

Enterprise T1203 Exploitation for Client Execution

Ramsay has been embedded in documents exploiting CVE-2017-0199, CVE-2017-11882, and CVE-2017-8570.[1][2]

Enterprise T1083 File and Directory Discovery

Ramsay can collect directory and file lists.[1][2]

Enterprise T1574 .001 Hijack Execution Flow: DLL

Ramsay can hijack outdated Windows application dependencies with malicious versions of its own DLL payload.[1]

Enterprise T1559 .001 Inter-Process Communication: Component Object Model

Ramsay can use the Windows COM API to schedule tasks and maintain persistence.[1]

.002 Inter-Process Communication: Dynamic Data Exchange

Ramsay has been delivered using OLE objects in malicious documents.[1]

Enterprise T1680 Local Storage Discovery

Ramsay can detect system information--including disk names, total space, and remaining space--to create a hardware profile GUID which acts as a system identifier for operators.[1][2]

Enterprise T1036 Masquerading

Ramsay has masqueraded as a JPG image file.[1]

.005 Match Legitimate Resource Name or Location

Ramsay has masqueraded as a 7zip installer.[1][2]

Enterprise T1106 Native API

Ramsay can use Windows API functions such as `WriteFile`, `CloseHandle`, and `GetCurrentHwProfile` during its collection and file storage operations. Ramsay can execute its embedded components via `CreateProcessA` and `ShellExecute`.[1]

Enterprise T1046 Network Service Discovery

Ramsay can scan for systems that are vulnerable to the EternalBlue exploit.[1][2]

Enterprise T1135 Network Share Discovery

Ramsay can scan for network drives which may contain documents for collection.[1][2]

Enterprise T1027 Obfuscated Files or Information

Ramsay has base64-encoded its portable executable and hidden itself under a JPG header. Ramsay can also embed information within document footers.[1]

.003 Steganography

Ramsay has PE data embedded within JPEG files contained within Word documents.[2]

Enterprise T1120 Peripheral Device Discovery

Ramsay can scan for removable media which may contain documents for collection.[1][2]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Ramsay has been distributed through spearphishing emails with malicious attachments.[2]

Enterprise T1057 Process Discovery

Ramsay can gather a list of running processes by using Tasklist.[2]

Enterprise T1055 .001 Process Injection: Dynamic-link Library Injection

Ramsay can use `ImprovedReflectiveDLLInjection` to deploy components.[1]

Enterprise T1091 Replication Through Removable Media

Ramsay can spread itself by infecting other portable executable files on removable drives.[1]

Enterprise T1014 Rootkit

Ramsay has included a rootkit to evade defenses.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Ramsay can schedule tasks via the Windows COM API to maintain persistence.[1]

Enterprise T1113 Screen Capture

Ramsay can take screenshots every 30 seconds as well as when an external removable storage device is connected.[2]

Enterprise T1016 System Network Configuration Discovery

Ramsay can use ipconfig and Arp to collect network configuration information, including routing information and ARP tables.[2]

Enterprise T1049 System Network Connections Discovery

Ramsay can use `netstat` to enumerate network connections.[2]

Enterprise T1080 Taint Shared Content

Ramsay can spread itself by infecting other portable executable files on networks shared drives.[1]

Enterprise T1204 .002 User Execution: Malicious File

Ramsay has been executed through malicious e-mail attachments.[2]
