Grandoreiro, Software S0531 | MITRE ATT&CK®

Archived: 2026-04-05 13:23:26 UTC

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

Grandoreiro can bypass UAC by registering as the default handler for .MSC files.[2]

Enterprise T1087 .003 Account Discovery: Email Account

Grandoreiro can parse Outlook .pst files to extract e-mail addresses.[2]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Grandoreiro has the ability to use HTTP in C2 communications.[3][2]

Enterprise T1010 Application Window Discovery

Grandoreiro can identify installed security tools based on window names.[2]

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

Grandoreiro can use run keys and create link files in the startup folder for persistence.[3][2]

.009 Boot or Logon Autostart Execution: Shortcut Modification

Grandoreiro can write or modify browser shortcuts to enable launching of malicious browser extensions.[3]

Enterprise T1185 Browser Session Hijacking

Grandoreiro can monitor browser activity for online banking actions and display full-screen overlay images to block user access to the intended site or present additional data fields.[1][3][2]

Enterprise T1115 Clipboard Data

Grandoreiro can capture clipboard data from a compromised host.[3]

Enterprise T1059 .005 Command and Scripting Interpreter: Visual Basic

Grandoreiro can use VBScript to execute malicious code.[1][2]

Enterprise T1555 .003 Credentials from Password Stores: Credentials from Web Browsers

Grandoreiro can steal cookie data and credentials from Google Chrome.[3][2]

Enterprise T1140 Deobfuscate/Decode Files or Information

Grandoreiro can decrypt its encrypted internal strings.[2]

Enterprise T1189 Drive-by Compromise

Grandoreiro has used compromised websites and Google Ads to bait victims into downloading its installer.[1][3]

Enterprise T1568 .002 Dynamic Resolution: Domain Generation Algorithms

Grandoreiro can use a DGA for hiding C2 addresses, including use of an algorithm with a user-specific key that changes daily.[1][2]

Enterprise T1573 .002 Encrypted Channel: Asymmetric Cryptography

Grandoreiro can use SSL in C2 communication.[3]

Enterprise T1041 Exfiltration Over C2 Channel

Grandoreiro can send data it retrieves to the C2 server.[2]

Enterprise T1222 .001 File and Directory Permissions Modification: Windows File and Directory Permissions Modification

Grandoreiro can modify the binary ACL to prevent security tools from running.[2]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

Grandoreiro can hook APIs, kill processes, break file system paths, and change ACLs to prevent security tools from running.[2]

.004 Impair Defenses: Disable or Modify System Firewall

Grandoreiro can block the Deibold Warsaw GAS Tecnologia security tool at the firewall level.[2]

.013 Impair Defenses: Disable or Modify Network Device Firewall

Grandoreiro can block the Deibold Warsaw GAS Tecnologia security tool at the firewall level. [2]

Enterprise T1070 .004 Indicator Removal: File Deletion

Grandoreiro can delete .LNK files created in the Startup folder.[2]

Enterprise T1105 Ingress Tool Transfer

Grandoreiro can download its second stage from a hardcoded URL within the loader's code.[3][2]

Enterprise T1056 .001 Input Capture: Keylogging

Grandoreiro can log keystrokes on the victim's machine.[2]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

Grandoreiro has named malicious browser extensions and update files to appear legitimate.[3][2]

Enterprise T1112 Modify Registry

Grandoreiro can modify the Registry to store its configuration at `HKCU\Software\` under frequently changing names including `%USERNAME%` and `ToolTech-RM`.[2]

Enterprise T1106 Native API

Grandoreiro can execute through the `WinExec` API.[2]

Enterprise T1027 .001 Obfuscated Files or Information: Binary Padding

Grandoreiro has added BMP images to the resources section of its Portable Executable (PE) file increasing each binary to at least 300MB in size.[2]

.011 Obfuscated Files or Information: Fileless Storage

Grandoreiro can store its configuration in the Registry at `HKCU\Software\` under frequently changing names including `%USERNAME%` and `ToolTech-RM`.[2]

.013 Obfuscated Files or Information: Encrypted/Encoded File

The Grandoreiro payload has been delivered encrypted with a custom XOR-based algorithm and also as a base64-encoded ZIP file.[1][2][2]

Enterprise T1566 .002 Phishing: Spearphishing Link

Grandoreiro has been spread via malicious links embedded in e-mails.[3][2]

Enterprise T1057 Process Discovery

Grandoreiro can identify installed security tools based on process names.[2]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

Grandoreiro can list installed security products including the Trusteer and Diebold Warsaw GAS Tecnologia online banking protections.[2][2]

Enterprise T1176 .001 Software Extensions: Browser Extensions

Grandoreiro can use malicious browser extensions to steal cookies and other user information.[3]

Enterprise T1539 Steal Web Session Cookie

Grandoreiro can steal the victim's cookies to use for duplicating the active session from another device.[3]

Enterprise T1218 .007 System Binary Proxy Execution: Msiexec

Grandoreiro can use MSI files to execute DLLs.[1]

Enterprise T1082 System Information Discovery

Grandoreiro can collect the computer name and OS version from a compromised host.[2]

Enterprise T1016 System Network Configuration Discovery

Grandoreiro can determine the IP and physical location of the compromised host via IPinfo.[2]

Enterprise T1033 System Owner/User Discovery

Grandoreiro can collect the username from the victim's machine.[2]

Enterprise T1124 System Time Discovery

Grandoreiro can determine the time on the victim machine via IPinfo.[2]

Enterprise T1204 .001 User Execution: Malicious Link

Grandoreiro has used malicious links to gain execution on victim machines.[3][2]

.002 User Execution: Malicious File

Grandoreiro has infected victims via malicious attachments.[3]

Enterprise T1497 .001 Virtualization/Sandbox Evasion: System Checks

Grandoreiro can detect VMWare via its I/O port and Virtual PC via the `vpcext` instruction.[2]

Enterprise T1102 .001 Web Service: Dead Drop Resolver

Grandoreiro can obtain C2 information from Google Docs.[1]

.002 Web Service: Bidirectional Communication

Grandoreiro can utilize web services including Google sites to send and receive C2 data.[3][2]
