BRONZE BUTLER, REDBALDKNIGHT, Tick, Group G0060

Archived: 2026-04-05 14:26:34 UTC

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

BRONZE BUTLER has used a Windows 10 specific tool and xxmm to bypass UAC for privilege escalation.[2][3]

Enterprise T1087 .002 Account Discovery: Domain Account

BRONZE BUTLER has used `net user /domain` to identify account information.[2]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

BRONZE BUTLER malware has used HTTP for C2.[2]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

BRONZE BUTLER has compressed data into password-protected RAR archives prior to exfiltration.[2][3]

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

BRONZE BUTLER has used a batch script that adds a Registry Run key to establish malware persistence.[2]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

BRONZE BUTLER has used PowerShell for execution.[2]

.003 Command and Scripting Interpreter: Windows Command Shell

BRONZE BUTLER has used batch scripts and the command-line interface for execution.[2]

.005 Command and Scripting Interpreter: Visual Basic

BRONZE BUTLER has used VBS and VBE scripts for execution.[2][3]

.006 Command and Scripting Interpreter: Python

BRONZE BUTLER has made use of Python-based remote access tools.[3]

Enterprise T1132 .001 Data Encoding: Standard Encoding

Several BRONZE BUTLER tools encode data with base64 when posting it to a C2 server.[2]

Enterprise T1005 Data from Local System

BRONZE BUTLER has exfiltrated files stolen from local systems.[2]

Enterprise T1039 Data from Network Shared Drive

BRONZE BUTLER has exfiltrated files stolen from file shares.[2]

Enterprise T1140 Deobfuscate/Decode Files or Information

BRONZE BUTLER downloads encoded payloads and decodes them on the victim.[2]

Enterprise T1189 Drive-by Compromise

BRONZE BUTLER compromised three Japanese websites using a Flash exploit to perform watering hole attacks.[4]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

BRONZE BUTLER has used RC4 encryption (for Datper malware) and AES (for xxmm malware) to obfuscate HTTP traffic. BRONZE BUTLER has also used a tool called RarStar that encodes data with a custom XOR algorithm when posting it to a C2 server.[2]

Enterprise T1203 Exploitation for Client Execution

BRONZE BUTLER has exploited Microsoft Office vulnerabilities CVE-2014-4114, CVE-2018-0802, and CVE-2018-0798 for execution.[4][3]

Enterprise T1083 File and Directory Discovery

BRONZE BUTLER has collected a list of files from the victim and uploaded it to its C2 server, and then created a new list of specific files to steal.[2]

Enterprise T1574 .001 Hijack Execution Flow: DLL

BRONZE BUTLER has used legitimate applications to side-load malicious DLLs.[3]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

BRONZE BUTLER has incorporated code into several tools that attempts to terminate anti-virus processes.[3]

Enterprise T1070 .004 Indicator Removal: File Deletion

The BRONZE BUTLER uploader or malware the uploader uses `command` to delete the RAR archives after they have been exfiltrated.[2]

Enterprise T1105 Ingress Tool Transfer

BRONZE BUTLER has used various tools to download files, including DGet (a similar tool to wget).[2]

Enterprise T1036 Masquerading

BRONZE BUTLER has masked executables with document file icons including Word and Adobe PDF.[3]

.002 Right-to-Left Override

BRONZE BUTLER has used Right-to-Left Override to deceive victims into executing several strains of malware.[3]

.005 Match Legitimate Resource Name or Location

BRONZE BUTLER has given malware the same name as an existing file on the file share server to cause users to unwittingly launch and install the malware on additional systems.[2]

Enterprise T1027 .001 Obfuscated Files or Information: Binary Padding

BRONZE BUTLER downloader code has included "0" characters at the end of the file to inflate the file size in a likely attempt to evade anti-virus detection.[2][3]

.003 Obfuscated Files or Information: Steganography

BRONZE BUTLER has used steganography in multiple operations to conceal malicious payloads.[3]

Enterprise T1588 .002 Obtain Capabilities: Tool

BRONZE BUTLER has obtained and used open-source tools such as Mimikatz, gsecdump, and Windows Credential Editor.[4]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

BRONZE BUTLER has used various tools (such as Mimikatz and WCE) to perform credential dumping.[2]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

BRONZE BUTLER used spearphishing emails with malicious Microsoft Word attachments to infect victims.[4][3]

Enterprise T1018 Remote System Discovery

BRONZE BUTLER typically use `ping` and Net to enumerate systems.[2]

Enterprise T1053 .002 Scheduled Task/Job: At

BRONZE BUTLER has used at to register a scheduled task to execute malware during lateral movement.[2]

.005 Scheduled Task/Job: Scheduled Task

BRONZE BUTLER has used schtasks to register a scheduled task to execute malware during lateral movement.[2]

Enterprise T1113 Screen Capture

BRONZE BUTLER has used a tool to capture screenshots.[2][3]

Enterprise T1518 Software Discovery

BRONZE BUTLER has used tools to enumerate software installed on an infected host.[3]

Enterprise T1007 System Service Discovery

BRONZE BUTLER has used TROJ_GETVERSION to discover system services.[3]

Enterprise T1124 System Time Discovery

BRONZE BUTLER has used `net time` to check the local time on a target system.[2]

Enterprise T1080 Taint Shared Content

BRONZE BUTLER has placed malware on file shares and given it the same name as legitimate documents on the share.[2]

Enterprise T1550 .003 Use Alternate Authentication Material: Pass the Ticket

BRONZE BUTLER has created forged Kerberos Ticket Granting Ticket (TGT) and Ticket Granting Service (TGS) tickets to maintain administrative access.[2]

Enterprise T1204 .002 User Execution: Malicious File

BRONZE BUTLER has attempted to get users to launch malicious Microsoft Word attachments delivered via spearphishing emails.[4][3]

Enterprise T1102 .001 Web Service: Dead Drop Resolver

BRONZE BUTLER's MSGET downloader uses a dead drop resolver to access malicious payloads.[2]
