GROUPS

BRONZE BUTLER

BRONZE BUTLER is a cyber espionage group with likely Chinese origins that has been active since at least 2008. The group primarily targets Japanese organizations, particularly those in government, biotechnology, electronics manufacturing, and industrial chemistry. [1] [2]

ID: G0060
Associated Groups: REDBALDKNIGHT, Tick
Version: 1.0
Created: 16 January 2018
Last Modified: 22 March 2019

Associated Group Descriptions

Name	Description
REDBALDKNIGHT	[1]
Tick	[1] [3]

Techniques Used

ATT&CK® Navigator Layers

Domain	ID	Name	Use
Enterprise	T1087	Account Discovery	BRONZE BUTLER has used `net user /domain` to identify account information.[2]
Enterprise	T1009	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]
Enterprise	T1088	Bypass User Account Control	BRONZE BUTLER malware xxmm contains a UAC bypass tool for privilege escalation.[2]
Enterprise	T1059	Command-Line Interface	BRONZE BUTLER uses the command-line interface.[2]
Enterprise	T1003	Credential Dumping	BRONZE BUTLER has used various tools to perform credential dumping.[2]
Enterprise	T1024	Custom Cryptographic Protocol	BRONZE BUTLER has used a tool called RarStar that encodes data with a custom XOR algorithm when posting it to a C2 server.[2]
Enterprise	T1002	Data Compressed	BRONZE BUTLER has compressed data into password-protected RAR archives prior to exfiltration.[2]
Enterprise	T1132	Data Encoding	Several BRONZE BUTLER tools encode data with base64 when posting it to a C2 server.[2]
Enterprise	T1022	Data Encrypted	BRONZE BUTLER has compressed and encrypted data into password-protected RAR archives prior to exfiltration.[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.[3]
Enterprise	T1203	Exploitation for Client Execution	BRONZE BUTLER has exploited Microsoft Word vulnerability CVE-2014-4114 for execution.[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	T1107	File Deletion	The BRONZE BUTLER uploader or malware the uploader uses `command` to delete the RAR archives after they have been exfiltrated.[2]
Enterprise	T1036	Masquerading	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	T1097	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	T1086	PowerShell	BRONZE BUTLER has used PowerShell for execution.[2]

Domain	ID	Name	Use
Enterprise	T1060	Registry Run Keys / Startup Folder	BRONZE BUTLER has used a batch script that adds a Registry Run key to establish malware persistence.[2]
Enterprise	T1105	Remote File Copy	BRONZE BUTLER has used various tools to download files, including DGet (a similar tool to wget).[2]
Enterprise	T1018	Remote System Discovery	BRONZE BUTLER typically use `ping` and Net to enumerate systems.[2]
Enterprise	T1053	Scheduled Task	BRONZE BUTLER has used at and 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]
Enterprise	T1064	Scripting	BRONZE BUTLER has used VBS, VBE, and batch scripts for execution.[2]
Enterprise	T1193	Spearphishing Attachment	BRONZE BUTLER used spearphishing emails with malicious Microsoft Word attachments to infect victims.[3]
Enterprise	T1071	Standard Application Layer Protocol	BRONZE BUTLER malware has used HTTP for C2.[2]
Enterprise	T1032	Standard Cryptographic Protocol	BRONZE BUTLER has used RC4 encryption (for Datper malware) and AES (for xxmm malware) to obfuscate HTTP traffic.[2]
Enterprise	T1124	System Time Discovery	BRONZE BUTLER has used `net time` to check the local time on a target system.[2]
Enterprise	T1204	User Execution	BRONZE BUTLER has attempted to get users to launch malicious Microsoft Word attachments delivered via spearphishing emails.[3]
Enterprise	T1102	Web Service	BRONZE BUTLER's MSGET downloader uses a dead drop resolver to access malicious payloads.[2]

Software

ID	Name	References	Techniques
S0110	at	[2]	Scheduled Task
S0106	cmd	[2]	Command-Line Interface, File and Directory Discovery, File Deletion, Remote File Copy, System Information Discovery
S0187	Daserf	[1] [3]	Code Signing, Command-Line Interface, Credential Dumping, Data Compressed, Data Encoding, Data Encrypted, Data Obfuscation, Indicator Removal from Tools, Input Capture, Masquerading, Obfuscated Files or Information, Remote File Copy, Screen Capture, Software Packing, Standard Application Layer Protocol, Standard Cryptographic Protocol
S0008	gsecdump	[2] [3]	Credential Dumping
S0002	Mimikatz	[2] [3]	Account Manipulation, Credential Dumping, Credentials in Files, DCShadow, Pass the Hash, Pass the Ticket, Private Keys, Security Support Provider, SID-History Injection
S0039	Net	[2]	Account Discovery, Create Account, Network Share Connection Removal, Network Share Discovery, Password Policy Discovery, Permission Groups Discovery, Remote System Discovery, Service Execution, System Network Connections Discovery, System Service Discovery, System Time Discovery, Windows Admin Shares
S0111	schtasks	[2]	Scheduled Task
S0005	Windows Credential Editor	[2] [3]	Credential Dumping

References

1. Chen, J. and Hsieh, M. (2017, November 7). REDBALDKNIGHT/BRONZE BUTLER's Daserf Backdoor Now Using Steganography. Retrieved December 27, 2017.
2. Counter Threat Unit Research Team. (2017, October 12). BRONZE BUTLER Targets Japanese Enterprises. Retrieved January 4, 2018.
3. DiMaggio, J. (2016, April 28). Tick cyberespionage group zeros in on Japan. Retrieved July 16, 2018.

MITRE

© 2015-2020, The MITRE Corporation. MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.

Privacy Policy

Terms of Use

ATT&CK v6.3

@MITREattack

Contact