Inception

attack.mitre.org/groups/G0100/

Inception is a cyber espionage group active since at least 2014. The group has targeted multiple industries and governmental entities primarily in Russia, but has also been active in the United States and throughout Europe, Asia, Africa, and the Middle East.[1][2][3]

ID: G0100

ⓘ

Associated Groups: Inception Framework, Cloud Atlas

Contributors: Oleg Skulkin, Group-IB

Version: 1.1

Created: 08 May 2020

Last Modified: 12 October 2021

Version Permalink
Live Version

Associated Group Descriptions

Name	Description
Inception Framework	[2]
Cloud Atlas	[3]

Techniques Used

Domain	ID	Name	Use	
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Inception has used HTTP, HTTPS, and WebDav in network communications.[3][1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Inception has maintained persistence by modifying Registry run key value `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\` .[3]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	Inception has used PowerShell to execute malicious commands and payloads.[1][3]
		.005	Command and Scripting Interpreter: Visual Basic	Inception has used VBScript to execute malicious commands and payloads.[1][3]

Domain	ID	Name	Use	
Enterprise	T1555	.003	Credentials from Password Stores: Credentials from Web Browsers	Inception used a browser plugin to steal passwords and sessions from Internet Explorer, Chrome, Opera, Firefox, Torch, and Yandex.[2]
Enterprise	T1005	Data from Local System	Inception used a file hunting plugin to collect .txt, .pdf, .xls or .doc files from the infected host.[4]	
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	Inception has encrypted network communications with AES.[3]
Enterprise	T1203	Exploitation for Client Execution	Inception has exploited CVE-2012-0158, CVE-2014-1761, CVE-2017-11882 and CVE-2018-0802 for execution.[4][3][2][1]	
Enterprise	T1083	File and Directory Discovery	Inception used a file listing plugin to collect information about file and directories both on local and remote drives.[2]	
Enterprise	T1027	Obfuscated Files or Information	Inception has encrypted malware payloads dropped on victim machines with AES and RC4 encryption.[3]	
Enterprise	T1588	.002	Obtain Capabilities: Tool	Inception has obtained and used open-source tools such as LaZagne.[4]
Enterprise	T1069	.002	Permission Groups Discovery: Domain Groups	Inception has used specific malware modules to gather domain membership.[2]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	Inception has used weaponized documents attached to spearphishing emails for reconnaissance and initial compromise.[3][2][1][4]
Enterprise	T1057	Process Discovery	Inception has used a reconnaissance module to identify active processes and other associated loaded modules.[2]	
Enterprise	T1090	.003	Proxy: Multi-hop Proxy	Inception used chains of compromised routers to proxy C2 communications between them and cloud service providers.[2]

Domain	ID	Name	Use
Enterprise	T1518	Software Discovery	Inception has enumerated installed software on compromised systems.[2]
Enterprise	T1218	.005	System Binary Proxy Execution: Mshta	Inception has used malicious HTA files to drop and execute malware.[4]
		.010	System Binary Proxy Execution: Regsvr32	Inception has ensured persistence at system boot by setting the value `regsvr32 %path%\ctfmonrn.dll /s` .[3]
Enterprise	T1082	System Information Discovery	Inception has used a reconnaissance module to gather information about the operating system and hardware on the infected host.[2]
Enterprise	T1221	Template Injection	Inception has used decoy documents to load malicious remote payloads via HTTP.[1]
Enterprise	T1204	.002	User Execution: Malicious File	Inception lured victims into clicking malicious files for machine reconnaissance and to execute malware.[3][4][2][1]
Enterprise	T1102	Web Service	Inception has incorporated at least five different cloud service providers into their C2 infrastructure including CloudMe.[3][2]

Software

ID	Name	References	Techniques
S0349	LaZagne	[4]	Credentials from Password Stores: Credentials from Web Browsers, Credentials from Password Stores, Credentials from Password Stores: Windows Credential Manager, Credentials from Password Stores: Keychain, OS Credential Dumping: LSASS Memory, OS Credential Dumping: Cached Domain Credentials, OS Credential Dumping: Proc Filesystem, OS Credential Dumping: LSA Secrets, OS Credential Dumping: /etc/passwd and /etc/shadow, Unsecured Credentials: Credentials In Files
S0441	PowerShower	[1]	Application Layer Protocol: Web Protocols, Archive Collected Data: Archive via Utility, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: Visual Basic, Command and Scripting Interpreter: PowerShell, Data Encoding: Standard Encoding, Exfiltration Over C2 Channel, Hide Artifacts: Hidden Window, Indicator Removal on Host: File Deletion, Modify Registry, Process Discovery, System Information Discovery, System Network Configuration Discovery, System Owner/User Discovery
S0442	VBShower	[4]	Application Layer Protocol: Web Protocols, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: Visual Basic, Indicator Removal on Host: File Deletion, Ingress Tool Transfer

References

Lancaster, T. (2018, November 5). Inception Attackers Target Europe with Year-old Office Vulnerability. Retrieved May 8, 2020. Symantec. (2018, March 14). Inception Framework: Alive and Well, and Hiding Behind Proxies. Retrieved May 8, 2020. GReAT. (2014, December 10). Cloud Atlas: RedOctober APT is back in style. Retrieved May 8, 2020. GReAT. (2019, August 12). Recent Cloud Atlas activity. Retrieved May 8, 2020.