

# Inception, Inception Framework, Cloud Atlas, Group G0100

Archived: 2026-04-05 15:05:09 UTC

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. [\[1\]\[3\]](#)

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 .013 Obfuscated Files or Information: Encrypted/Encoded File](#)

[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](#).<sup>[4]</sup>

Enterprise [T1069 .002 Permission Groups Discovery: Domain Groups](#)

[Inception](#) has used specific malware modules to gather domain membership.<sup>[2]</sup>

Enterprise [T1566 .001 Phishing: Spearphishing Attachment](#)

[Inception](#) has used weaponized documents attached to spearphishing emails for reconnaissance and initial compromise.<sup>[3][2][1][4]</sup>

Enterprise [T1057 Process Discovery](#)

[Inception](#) has used a reconnaissance module to identify active processes and other associated loaded modules.<sup>[2]</sup>

Enterprise [T1090 .003 Proxy: Multi-hop Proxy](#)

[Inception](#) used chains of compromised routers to proxy C2 communications between them and cloud service providers.<sup>[2]</sup>

Enterprise [T1518 Software Discovery](#)

[Inception](#) has enumerated installed software on compromised systems.<sup>[2]</sup>

Enterprise [T1218 .005 System Binary Proxy Execution: Mshta](#)

[Inception](#) has used malicious HTA files to drop and execute malware.<sup>[4]</sup>

[.010 System Binary Proxy Execution: Regsvr32](#)

[Inception](#) has ensured persistence at system boot by setting the value `regsvr32 %path%\ctfmonrn.dll /s`.<sup>[3]</sup>

Enterprise [T1082 System Information Discovery](#)

[Inception](#) has used a reconnaissance module to gather information about the operating system and hardware on the infected host.<sup>[2]</sup>

Enterprise [T1221 Template Injection](#)

[Inception](#) has used decoy documents to load malicious remote payloads via HTTP.<sup>[1]</sup>

Enterprise [T1204 .002 User Execution: Malicious File](#)

[Inception](#) lured victims into clicking malicious files for machine reconnaissance and to execute malware.<sup>[3][4][2][1]</sup>

Enterprise [T1102 Web Service](#)

[Inception](#) has incorporated at least five different cloud service providers into their C2 infrastructure including CloudMe. [\[3\]\[2\]](#)

---

Source: <https://attack.mitre.org/groups/G0100/>