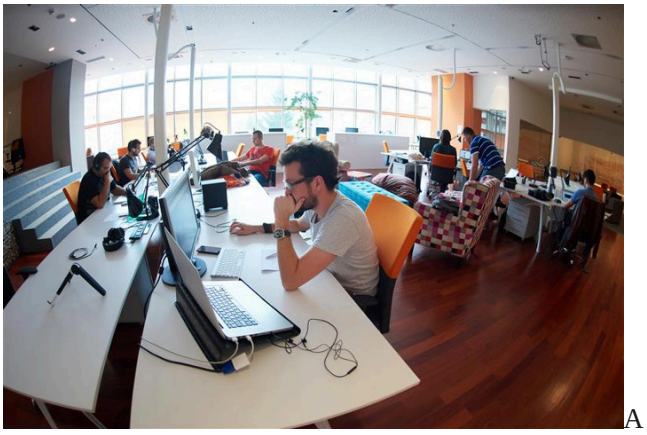
Cloud Atlas Group Updates Infection Chain With Polymorphic Malware to Evade Detection

Archived: 2026-04-05 21:14:55 UTC

 A malware campaign that uses a polymorphic HTML application (HTA) and a polymorphic backdoor to evade detection has recently been observed by security researchers. As reported by researchers at Kaspersky, the campaign can be traced to the advanced persistent threat (APT) group Cloud Atlas (aka Inception), whose activities were first reported in 2014 and have recently been identified in relation to attacks on various organizations in Russia, Central Asia, Europe, and Portugal.

As in its previous iteration, the routine used by Cloud Atlas begins with phishing emails to high-value targets. These emails have Microsoft Office document attachments that contain malicious remote templates, which are loaded from remote servers. This technique allows the documents to bypass static analysis and makes forensic analysis difficult if the servers hosting the templates are down.

In Cloud Atlas' updated infection chain, the templates, when downloaded, deliver and execute a malicious HTA that, in turn, drops and executes a VBScript module named VBShower, which is a polymorphic backdoor. VBShower deletes traces of infection from the machine to further complicate forensics and establishes the communication between the infected machine and the command-and-control (C&C) server.

[Read: Risks under the radar: Understanding fileless threatsnews article]

VBShower delivers Cloud Atlas' second-stage payload, a backdoor that uses WebDAV to communicate with a cloud storage service. More notably, VBShower also delivers a PowerShellnews article-based implant named PowerShower, which is the main payload in Cloud Atlas's previous routine. PowerShower deploys several modules. These include a PowerShell stealer that exfiltrates documents that are smaller than 5 MB and have been modified in the last two days, a reconnaissance module that retrieves a list of active processes and other system information, and a password grabber, based on the open-source tool LaZagne, that collects credentials stored in the infected system.

Both the HTA and VBShower are polymorphic, that is, they modify their attributes so as to avoid detection by security solutions. In particular, the updated infection chain's polymorphism allows Cloud Atlas to evade analysis

based on indicators of compromise (IOCs), since the code in both modules will be unique for every infected machine.

Polymorphism and PowerShell abuse for malware propagation and infection are not new. Threat actors have been abusing new scripting languages, for example, to make it difficult for enterprise IT teams to seek, monitor, and defend against these threats. Trend Micro researchers have been tracking such evasion and infection techniques.

[Read: Security 101: Defending against fileless malwarenews article]

Infections such as those carried out by Cloud Atlas' updated routine not only pose threats to users whose credentials and information are compromised. They also give malicious actors access even after the initial infection phase, with the backdoor components enabling them to perform more serious attacks.

Here are some best practices for users and enterprises to follow so as to defend their systems against these threats:

- Update and install the latest patches released. Legacy systems can use virtual patches released by security vendors to protect unsupported systems.
- Be wary of emails from unknown senders or locations, or messages with suspicious contentnews-cybercrime-and-digital-threats even from supposed known senders.
- Disable unnecessary and outdated components, and proactively monitor systems and networks for unusual activities and increased outbound traffic.
- Install a multilayered protection system capable of behavior monitoring to detect and block anomalies from malware infection and software modifications, from the gateway to the endpoint.

Trend Micro solutions

Trend Micro's Smart Protection Suites deliver several capabilities like high-fidelity machine learning and web reputation services that minimize the impact of persistent, fileless threats. The Trend Micro™ Deep Discovery™ solution has a layer for email inspectionproducts that can protect enterprises by detecting malicious attachments and URLs. It can detect remote scripts even if they are not being downloaded on the physical endpoints.

We Recommend

- The Industrialization of Botnets: Automation and Scale as a New Threat Infrastructurenews article
- Complexity and Visibility Gaps in Power Automatenews article
- Cracking the Isolation: Novel Docker Desktop VM Escape Techniques Under WSL2news article
- Azure Control Plane Threat Detection With TrendAI Vision One™news article
- The AI-fication of Cyberthreats: Trend Micro Security Predictions for 2026predictions
- Ransomware Spotlight: DragonForcenews article
- Stay Ahead of AI Threats: Secure LLM Applications With Trend Vision Onenews article
- The Road to Agentic AI: Navigating Architecture, Threats, and Solutionsnews article

---