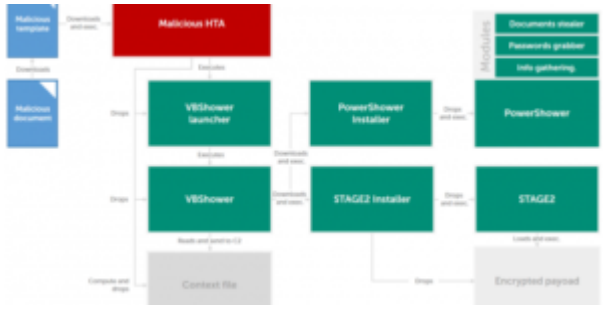
Cloud Atlas APT upgrades its arsenal with polymorphic malware



Cloud Atlas, an advanced persistent threat (APT), also known as Inception, has updated its attack arsenal with new tools which allow it to avoid detection through standard Indicators of Compromise. This updated infection chain has been spotted in the wild in different organizations in Eastern Europe, Central Asia and Russia.

Cloud Atlas is a threat actor that has a long history of cyber-espionage operations targeting industries,
government agencies and other entities. It was first identified in 2014 and has been active ever since.

Recently, Kaspersky researchers have seen Cloud Atlas targeting the international economics and aerospace industries as well as governmental and religious organizations in Portugal, Romania, Turkey,
Ukraine, Russia, Turkmenistan, Afghanistan and Kyrgyzstan among other countries. Upon successful infiltration, Cloud Atlas would:

 collect information about the system to which it has gained access
 log passwords
 exfiltrate recent .txt .pdf. xls .doc files to a command and control server.

While Cloud Atlas hasn’t dramatically changed its tactics, since 2018, recent waves of attacks research
has discovered it has started to implement a novel way of infecting its victims and conducts lateral movement through their network.

Fig.1: The infection chain that was used by Cloud Atlas before April 2019.

Previously, Cloud Atlas would first send a spear-phishing email with a malicious attachment to a target.

In the case of a successful exploitation, PowerShower – the attached malware, used for initial reconnaissance and to download additional malicious modules – would then be executed to allow cyberattackers to proceed with an operation.

The newly updated chain of infection postpones the execution of PowerShower until a later stage; instead, after the initial infection, a malicious HTML app is now downloaded and executed on the

target
machine. This application will then collect initial information about the attacked computer, and download
and execute VBShower – another malicious module. VBShower then erases evidence of the presence of malware in the system and consults with its masters through command and control servers, to decide
on further actions. Depending on the command received, this malware will then download and execute
either PowerShower or another well-known Cloud Atlas' second stage backdoor.

Cloud Atlas APT upgrades its arsenal with polymorphic malware
Fig 2. The updated Cloud Atlas infection chain
While this new infection chain is in general much more complicated than the previous model, its main
differentiator is the fact that a malicious HTML application and the VBShower module are polymorphic.
This means that the code in both modules will be new and unique in each case of infection. According to
Kaspersky experts, this updated version is carried out in order to make the malware invisible to security
solutions relying on familiar Indicators of Compromise.
"It has become good practice in the security community to share the Indicators of Compromise (IoC) of
malicious operations we find through research. This practice allows us to respond to ongoing international cyber-espionage operations quite swiftly, preventing any further damage they could cause.
However, as we predicted as early as 2016, IoC have become obsolete as a reliable tool to spot a targeted attack in your network. This first emerged with ProjectSauron, which would create a unique set
of IoC for each of its victims and continued with the trend of using open source tools in espionage operations instead of unique ones. This is now continuing with this recent example of polymorphic malware. This doesn't mean that actors are becoming harder to catch, but that security skills and the
defenders toolkit needs to evolve along with the toolkit and skills of the malicious actors they are tracking," – said Felix Aime, security researcher in the Kaspersky Global Research and Analysis Team.
Kaspersky recommends that organizations use anti-targeted attack solutions enhanced with Indicators
of Attack (IoA) that focus on the tactics, techniques or actions that malefactors may take when preparing
for an attack. IoAs track the techniques deployed, no matter what specific tools are used. The latest versions of Kaspersky Endpoint Detection and Response, and Kaspersky Anti Targeted Attack both feature a new database of IoAs, maintained and updated by Kaspersky's own expert threat hunters.
The latest versions of Kaspersky EDR and Kaspersky Anti Targeted Attack offer new features that simplify the investigation process and enhance threat huntingThe latest versions of Kaspersky EDR and Kaspersky Anti Targeted Attack offer new features that simplify the investigation process and enhance threat huntingOther recommendations for organizations from Kaspersky:
 Educate your staff on digital hygiene and explain how they can recognize and avoid potentially malicious emails or links. Consider introducing dedicated awareness training for employees
 Use an endpoint security solution fitted with anti-spam and anti-phishing components, as well as application control functionality with a default deny mode to block the execution of unauthorized

applications — such as Kaspersky Endpoint Security for Business

Cloud Atlas APT upgrades its arsenal with polymorphic malware
 For endpoint level detection, investigation and timely remediation of incidents, implement an EDR solution such as Kaspersky Endpoint Detection and Response, to catch even unknown banking malware
 Implement a corporate-grade security solution that detects advanced threats on the network at an early stage, such as Kaspersky Anti Targeted Attack Platform
 Integrate threat intelligence into your Security Information and Event Management (SIEM) services
and security controls, in order to access the most relevant and up-to-date threat data.
Read the full text of the report on Securelist.com
About Kaspersky
Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and
security expertise is constantly transforming into innovative security solutions and services to protect
businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users
are protected by Kaspersky technologies and we help 270,000 corporate clients protect what matters
most to them. Learn more at www.kaspersky.com.