Inception Framework: Alive and Well, and Hiding Behind Proxies

symantec.com/blogs/threat-intelligence/inception-framework-hiding-behind-proxies

Espionage group has remained active over the past three years, using cloud and IoT to hide in plain sight.

The cyber espionage group known as the Inception Framework has significantly developed its operations over the past three years, rolling out stealthy new tools and cleverly leveraging the cloud and the Internet of Things (IoT) in order to make its activities harder to detect.

Since 2014, Symantec has found evidence of a steady stream of attacks from the Inception Framework targeted at organizations on several continents. As time has gone by, the group has become ever more secretive, hiding behind an increasingly complex framework of proxies and cloud services.

History of stealthy attacks

The Inception Framework has been active since at least May 2014 and its activities were first exposed by Blue Coat (now part of Symantec) in December 2014. Right from the start, the group stood out because of its use of an advanced, highly automated framework to support its targeted attacks. This level of sophistication is rarely seen, even in the targeted attacks sphere. The nature of Inception's targets, from 2014 right through to today, along with the capabilities of its tools, indicate that espionage is the primary motive of this groups

In 2014, Inception was compromising targeted organizations using spear-phishing emails, which masqueraded as legitimate emails concerning international policy, upcoming conferences, and specific sectoral interests of the targeted organization.

More than half of the group's earlier targets were in the Energy or Defense sectors, but it also targeted organizations in the Consultancy/Security, Aerospace, Research, and Media sectors, in addition to embassies. Its activities ranged across the globe, with targets located in South Africa, Kenya, the United Kingdom, Malaysia, Suriname, along with several other European and Middle Eastern countries.

Word documents attached to Inception's spear-phishing emails leveraged two Microsoft Office vulnerabilities (CVE-2014-1761 and CVE-2012-0158) to install malware on the recipient's computer. The malware had a multi-staged structure that began with a malicious RTF document and ended with an in-memory DLL payload that communicated, via the WebDAV protocol, with a command and control (C&C) address from a legitimate cloud service provider (CloudMe.com). The name "Inception" comes from the group's many levels of obfuscation and indirection it employed in delivering this payload.

Further layers of obfuscation emerged when Blue Coat was able to determine that the attackers were communicating with CloudMe.com through a hacked network of compromised routers, the majority of which were located in South Korea.

Stepping out of the shadows once again

Following its exposure in late 2014, Inception fell quiet. However, this turned out to be only a brief hiatus and, by April 2015, there had been a resurgence in activity. Attacks have continued since then, right through to 2017.

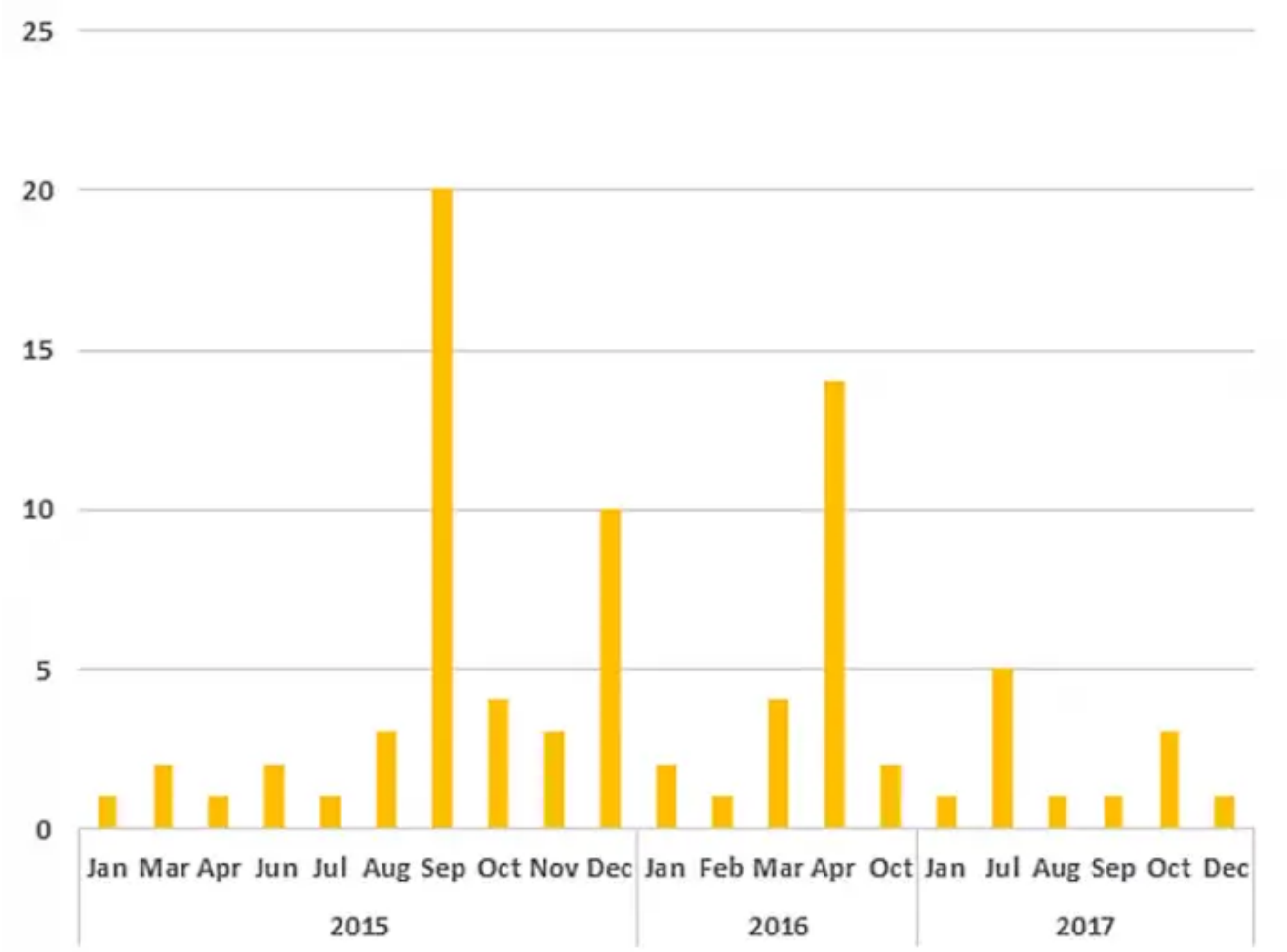

Figure 1. Inception Framework attacks 2015-2017

In the intervening years, the Inception Framework has evolved, adding additional layers of obfuscation in a bid to avoid detection. The group is using new types of lure documents in its spear-phishing campaigns and its malware has expanded to use new types of plugins. Inception has also increased its use of the cloud, and diversified the range of cloud providers it uses for C&C purposes.

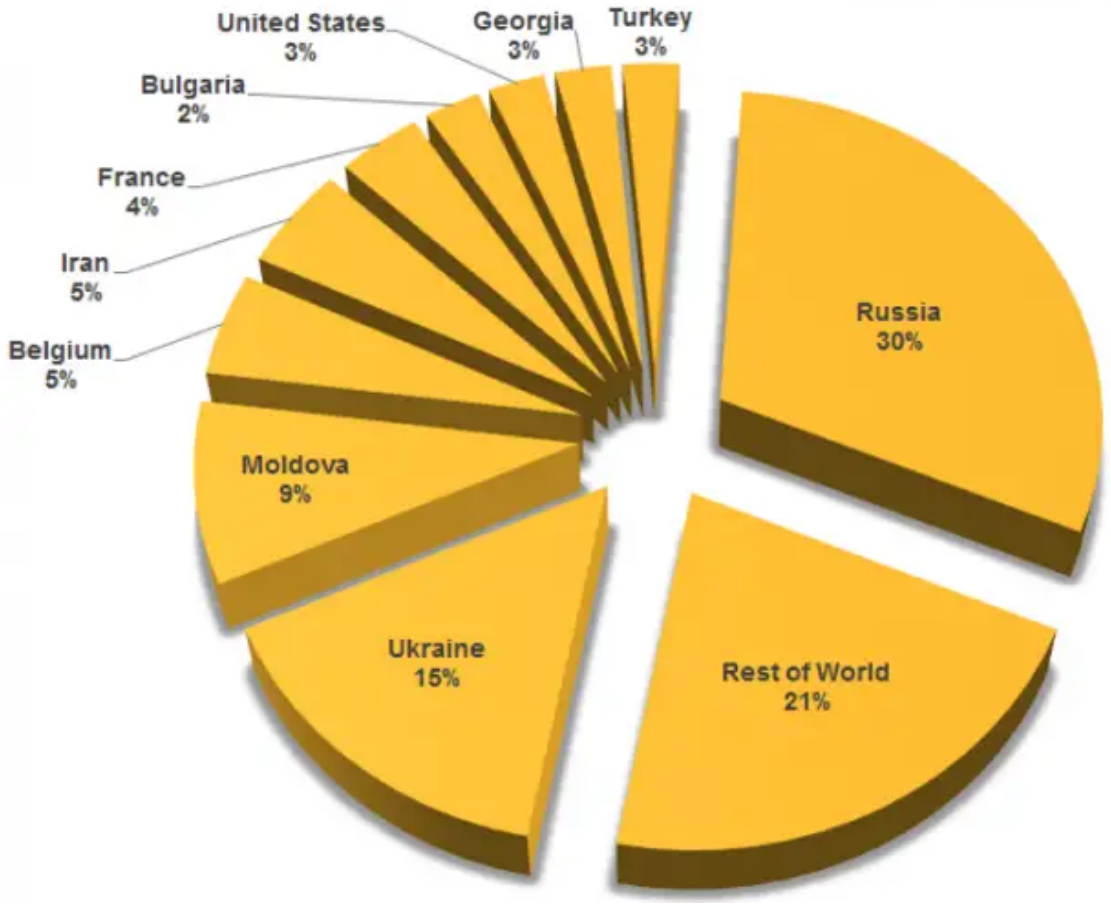

Figure 2. Locations of organizations targeted by Inception, 2015-2017
The locations of Inception's targets have shifted since 2014, but the group continues to have a global reach. Russia accounted for the largest number of attacks between 2015 and 2017, followed by Ukraine, Moldova, Belgium, Iran, and France.

An evolved attack framework

Since 2014, the Inception Framework has steadily changed its tools and techniques. In its early attacks, the group's malware payload (with the exception of plugins) was fully contained within an exploit document emailed to the victim. In more recent activity, these spear-phishing attacks are now a two-stage process. The group will first email the target a malicious "Reconnaissance document" which, if opened, will fingerprint the target computer, gathering information on what software it is running and whether that software is up to date.

Several days later, Inception will send a second spear-phishing email to the target, with another malicious document attached. This document is designed to retrieve a remote RTF file, which contains the exploit, and open it on the target's computer.

Shortly after this RTF document is opened, the remaining stages of the Inception malware are found executing on the system. The loader DLL is responsible for decrypting and injecting the core payload DLL into memory, from an encrypted file present on disk. The core

payload DLL's main function is to gather system information, execute other malware in the form of plugins, and update itself. It accesses C&C via WebDAV hosted on legitimate cloud storage providers.

The use of an initial reconnaissance document allows Inception to profile the target's computer and potentially customize any subsequent malicious document to exploit known vulnerabilities in unpatched software on the computer.

By breaking its attacks up into distinct stages, Inception also makes them harder to detect. For investigators to trace an attack, each stage will have be uncovered and referenced to the other stages.

Modular malware

Inception's malware is modular and the attackers will load plugins based on requirements for each attack. The group has used a range of plugins in recent attacks, some of which are improved versions of plugins used in 2014, while others were previously unseen.

- **File hunting plugin**: The most frequently used plugin, similar to one used in 2014. Often used to collect Office files from temporary internet history.
- **Detailed survey plugin:** Used to gather domain membership, processes/loaded modules, hardware enumeration, installed products, logical and mapped drive information. Evolution of earlier plugin used in 2014.
- **Browser plugin:** Used to steal browser history, stored passwords and sessions. Works with Internet Explorer, Chrome, Opera, Firefox, Torch, and Yandex.
- **File listing plugin:** Works on local or remote drives and can map additional paths when given credentials.

Expanding use of the cloud

Since 2014, Inception has widened its use of cloud service providers for C&C purposes. Whereas previously it relied on one service provider (CloudMe.com), more recently it has employed a least five cloud service providers

Leveraging the cloud for C&C has a number of advantages for groups like Inception. Any C&C communications will involve encrypted traffic to a known website, meaning it is less likely to raise flags on targeted networks. Legitimate cloud services are not likely to be blacklisted.

Varying the cloud service provider used adds a further degree of stealth. Once it became known Inception was using a single provider, any traffic to that provider may have attracted additional scrutiny.

Symantec has notified all cloud providers affected. Where possible Symantec has provided details on the C&C accounts used by Inception to the affected cloud providers. The accounts in questions have been deleted or disabled.

Using IoT to hide behind proxies

Inception is continuing to use chains of infected routers to act as proxies and mask communications between the attackers and the cloud service providers they use. Certain router manufacturers have UPnP listening on WAN as a default configuration. Akamai research has found that there are 765,000 devices vulnerable to this attack. These routers are hijacked by Inception and configured to forward traffic from one port to another host on the internet. Abuse of this service requires no custom malware to be injected on the routers and can be used at scale very easily. Inception strings chains of these routers together to create multiple proxies to hide behind.

"#InceptionFramework evolved, rolling out new tools & hiding behind increasingly complex array of proxies & cloud services symc.ly/2GsqXra"
Click to Tweet
Every connection builds different chains of infected routers and once the connection is complete, it cleans up after itself. In several cases, Symantec has been able to follow the entire chain of compromised routers and found it led to a virtual private server (VPS), meaning the attackers have employed an additional layer of security by routing communications through rented hosting servers.

Mobile devices targeted

Inception has an ongoing interest in mobile devices and has previously developed malware to infect Android (Android.Lastacloud), iOS (IOS.Lastaccoud) and BlackBerry devices (BBOS.Lastacloud).

Mobile malware continues to be deployed and the group has made some modifications to its Android malware. The malware is spread via SMS messages and emails containing malicious links. Once installed, it uses user profile pages on online forums as dead drops for its C&C.

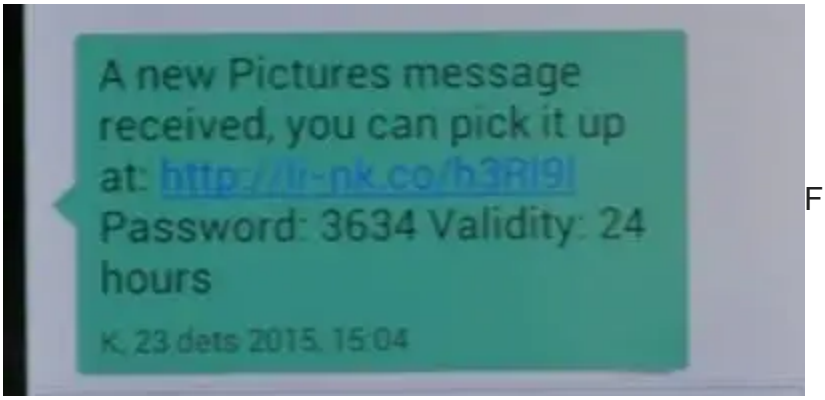

Figure 3. Malicious SMS message used by Inception to spread Android malware

Persistence, stealth, and global reach

Even prior to its discovery in 2014, Inception went to great lengths both to avoid detection and conceal its location. Exposure hasn't deterred the group. Instead, it has redoubled its efforts, adding more layers of obfuscation to an already complex attack framework. Its persistence, stealth, and global reach mean the group continues to pose an ongoing risk to organizations, particularly in its areas of interest, which include defense, aerospace, energy, governments, telecoms, media, and finance.

Aside from a suite of advanced modular malware, the group is notable for its ability to make use of new platforms such as the cloud, IoT, and mobile to facilitate its attacks. An "early adopter", Inception's tactics may point the way towards how other espionage groups may modify their methods in years to come.

Protection

Symantec has had protection for all of the Inception Framework tools since the initial emergence of the group in 2014. The following detections are in place today:

File-based protection

- Infostealer.Rodagose
- Trojan.Rodagose!g1
- Trojan.Rodagose!g2
- Trojan.MDropper

Mobile

- Android.Lastacloud

- BBOS.Lastacloud
- IOS.Lastacloud

Network Protection Products

Malware Analysis Appliance detects activity associated with Inception

Customers with Webpulse-enabled products are protected against activity associated with Inception

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.

About the Author

Network Protection Security Labs

Network Protection Security Labs is a group of security experts within Network Protection Products doing advanced security research to continuously improve Symantec Network Products.

Want to comment on this post?