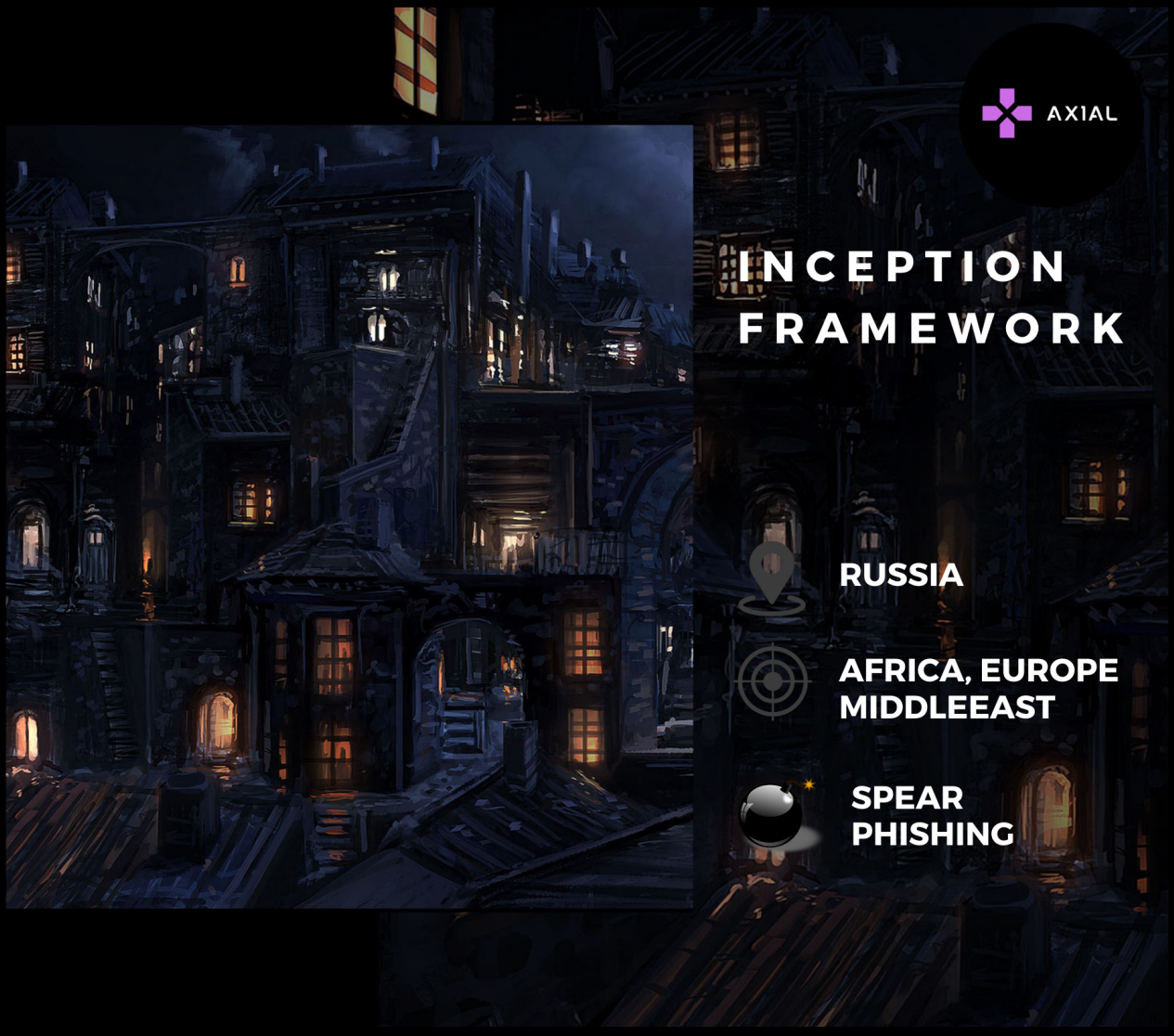
INCEPTION FRAMEWORK



HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON INCEPTION FRAMEWORK : ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Researchers from Blue Coat Labs have identified the emergence of a previously undocumented attack framework that is being used to launch highly targeted attacks in order to gain access to, and extract confidential information from, victims' computers. Because of the many layers used in the design of the malware, we've named it Inception—a reference to the 2010 movie "Inception" about a thief who entered peoples' dreams and stole secrets from their subconscious. Targets include individuals in strategic positions: Executives in important businesses such as oil, finance and engineering, military officers, embassy personnel and government officials. The Inception attacks began by focusing on targets primarily located in Russia or related to Russian interests, but have since spread to targets in other locations around the world. The preferred malware delivery method is via phishing emails containing trojanized documents.

II. TARGETS

Sectors: Aerospace, Defense, Embassies, Energy, Engineering, Financial, Government, Oil and gas, Research.
Countries:
Afghanistan, Armenia, Austria, Azerbaijan, Belarus, Belgium, Brazil, Congo, Cyprus, France, Georgia, Germany, Greece, India, Indonesia, Iran, Italy, Jordan, Kazakhstan, Kenya, Kyrgyzstan, Lebanon, Lithuania, Malaysia, Moldova, Morocco, Mozambique, Oman, Pakistan, Paraguay, Portugal, Qatar, Romania, Russia, Saudi Arabia, South Africa, Suriname, Switzerland, Tajikistan, Tanzania, Turkey, Turkmenistan, Uganda, Ukraine, UAE, USA, Uzbekistan, Venezuela, Vietnam.

III. TOOLS USED

Inception, Lastacloud, PowerShower, VBShower and many 0-day exploits

IV. CAMPAIGNS

Oct 2012
Operation “RedOctober”In October 2012, Kaspersky Lab’s Global Research & Analysis Team initiated a new threat research after a series of attacks against computer networks of various international diplomatic service agencies. A large scale cyber-espionage network was revealed and analyzed during the investigation, which we called “Red October” (after famous novel “The Hunt For The Red October”).

May 2014
Hiding Behind ProxiesSince 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.

Aug 2014
Operation “Cloud Atlas”In August 2014, some of our users observed targeted attacks with a variation of CVE-2012-0158 and an unusual set of malware. We did a quick analysis of the malware and it immediately stood out because of certain unusual things that are not very common in the APT world.

Oct 2018
This blog describes attacks against European targets observed in October 2018, using CVE-2017-11882 and a new PowerShell backdoor we’re calling POWERSHOWER due to the attention to detail in terms of cleaning up after itself, along with the malware being written in PowerShell.

2019
During its recent campaigns, Cloud Atlas used a new “polymorphic” infection chain relying no more on PowerShower directly after infection, but executing a polymorphic HTA hosted on a remote server, which is used to drop three different files on the local system.

VI. IOCS

1. 13de9678279b6ce6d81aeb32c0dd9f7458ad1f92aee17f3e052be9f06d473bed
2. 2bcb8a4ddc2150b25a44c292db870124c65687444f96e078f575da69bbf018e0
3. 49dbcf1fc8d3381e495089f396727a959885c1dd2ab6cd202cf3c4dbd1d27c4f
4. 687ee860fd5cd9902b441c26d72788d5a52052d03047a9b071808fc4c53a7e8b
5. 8aef4975d9c51821c4fa8ee1cbfe9c1f4a88c8784427d467ea99b2c1dabe15ae
6. 8b212ee2d65c4da033c39aebaf59cc51ade45f32f4d91d1daa0bd367889f934d
7. cc64a68ba52283f6cf5521cf75567b3c5b5143f324d37c59906ee63f1bbafcaf

C&C

1. 108.170.52.158
2. 188.165.62.40
3. 200.122.128.208
4. 51.255.139.194

VII. REFERENCES

1. https://www.akamai.com/uk/en/multimedia/documents/white-paper/upnproxy-blackhat-proxies-via-nat-injections-white-paper.pdf
2. https://pan-unit42.github.io/playbook_viewer/?pb=inception
3. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/inception-framework-hiding-behind-proxies
4. https://www.infosecurity-magazine.com/news/inception-apt-malware/
5. https://www.techrepublic.com/resource-library/webcasts/the-inception-framework-an-apt-campaign-in-the-cloud-mobile-and-embedded-systems/
6. https://the-parallax.com/2018/03/20/inception-framework-apt-wifi-router/
7. https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/Inception_APT_Analysis_Bluecoat.pdf