Blue Coat Exposes “The Inception Framework”; Very Sophisticated, Layered Malware Attack Targeted at Military, Diplomats, and Business Execs

Share this:

Snorre Fagerland and Waylon Grange

December 9, 2014

- ***One of the most sophisticated malware attacks Blue Coat Labs has ever seen***
- ***Initially targeted at Russia, but expanding globally***
- ***Masterful identity cloaking and diversionary tactics***
- ***Clean and elegant code suggesting strong backing and top-tier talent***
- ***Includes malware targeting mobile devices: Android, Blackberry and iOS***
- ***Using a free cloud hosting service based in Sweden for command and control***

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.

Command & Control traffic on the Windows platform is performed indirectly via a Swedish cloud service provider using the WebDAV protocol. This hides the identity of the attacker and may bypass many current detection mechanisms.

The attackers have added another layer of indirection to mask their identity by leveraging a proxy network composed of routers, most of which are based in South Korea, for their command and control communication. It is believed that the attackers were able to compromise these devices based on poor configurations or default credentials.

Based on the multiple layers of obfuscation and indirection in the malware, along with the control mechanisms between attacker and target, it is clear the attackers behind Inception are intent on staying in the shadows.

The framework continues to evolve. Blue Coat Lab researchers have recently found that the attackers have also created malware for Android, BlackBerry and iOS devices to gather information from victims, as well as seemingly planned MMS phishing campaigns to mobile devices of targeted individuals. To date, Blue Coat has observed over 60 mobile providers such as China Mobile, O2, Orange, SingTel, T-Mobile and Vodafone, included in these preparations, but the real number is likely far higher.

Expanded details about Inception are also available via a new technical whitepaper, "The Inception Framework: Cloud-hosted APT."

Highly Targeted Attacks on Political, Military, Financial and Oil Industries

Initially, attacks campaigns seemed to be largely focused on Russia and a few other Eastern European countries. However, Blue Coat has also seen attacks on targets in other countries across the globe.

While information about targets is limited, Blue Coat researchers have uncovered a number of phishing emails highlighting industry targets:

Inception Framework: Attack Targets

- Finance [Russia]
- Oil industry [Romania, Venezuela, Mozambique]
- Embassies/Diplomacy [Paraguay, Romania, Turkey]

Researchers have also obtained decoy documents that indicate an interest in:

- Embassies
- Politics
- Finance
- Military
- Engineering

Initial Discovery

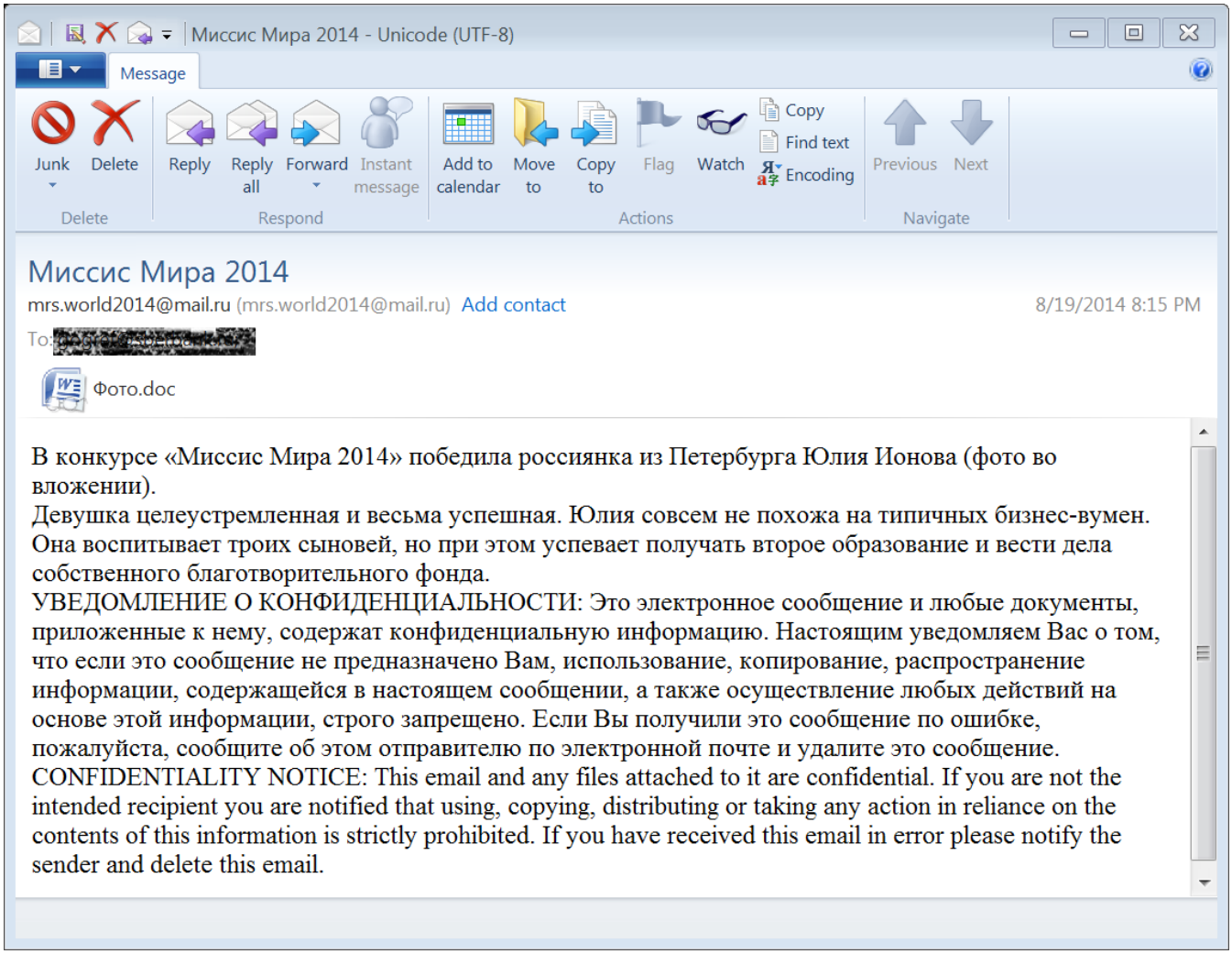
In March 2014, Microsoft published information about a new vulnerability in Rich Text Format (RTF). This vulnerability, named CVE-2014-1761 (Microsoft Word RTF Object Confusion), was already exploited by attackers. Two previous RTF vulnerabilities, CVE-2010-3333 and CVE-2012-0158, became mainstays of targeted attacks, so Blue Coat Lab researchers followed the usage this new exploit with interest.

In late August, Blue Coat identified a malware espionage operation that used both the CVE-2014-1761 and CVE-2012-0158 vulnerabilities to trigger execution of the malicious payload, and which leveraged a Swedish cloud service, CloudMe, as the backbone of its entire visible infrastructure.

When Blue Coat notified CloudMe.com about the abuse of their services, CloudMe was very helpful, providing further research, including a great deal of log information related to the attack. It must be noted that the CloudMe service is not actively spreading the malicious content; the attackers are only using it for storing their files.

How Does Inception Work?

Initial malware components have, in all cases that Blue Coat has observed, been embedded in Rich Text Format (RTF) files. Exploitation of vulnerabilities in this file format is leveraged to gain remote access to victim's computers. These files are delivered to the victim via phishing emails with exploited Word documents attached.



EXAMPLE of Phishing Email

Example of attached document, containing two exploit containers; one targeting CVE-2012-0158 (MSCOMCTL ActiveX Buffer Overflow), the other targeting CVE-2014-1761.

Example of attached document, containing two exploit containers; one targeting CVE-2012-0158 (MSCOMCTL ActiveX Buffer Overflow), the other targeting CVE-2014-1761.

When the user clicks on the attachment, a Word document is displayed to avoid arousing suspicion from the user while malicious content stored inside the document in encoded form writes to their disk. Unusual for many exploit campaigns, the names of the dropped files vary and have been clearly randomized in order to avoid detection by name.

The malware gathers system information from the infected machine, including OS version, computer name, user name, user group membership, the process it is running in, locale ID's, as well as system drive and volume information. All of this system information is encrypted and sent to cloud storage via WebDAV. The framework is designed in such a way that all communication after malware infection (i.e. target surveying, configuration updates, malware updates, and data exfiltration) can be performed via the cloud service.

The malware components of this framework follow a plug-in model, where new malware rely on already existing malware components to interact with the framework. Without the initial installer, none of the subsequent separate modules will work, and most of these will only exist in memory – vanishing at reboot.

The operational security exhibited by the attackers is among the most advanced that Blue Coat has witnessed. Most interaction between attackers and their infrastructure is performed via a convoluted network of router proxies and rented hosts, most likely compromised because of poor configurations or default credentials.

Attack Origins Masked by Obfuscation and Misdirection

The attackers have left a slew of potential hints to their physical location. However, it is extremely difficult to distinguish which of these indicators are legitimate clues and which are bread crumbs intentionally dropped to obscure their trail. Listed below are the indicators we have discovered and what conclusions *could* be drawn from each about the origins of the attacks.

Red Herrings

- In specific instances where the APT seemed to be under investigation by researchers the actors dropped another piece of malware that is clearly attributable to a previously known Chinese APT: Suggests ties to China
- A large majority of the hacked home routers are in South Korea: Suggests ties to South Korea
- The attackers are most active from 8:00AM to 5:00PM in the Eastern European Timezone: Suggests ties to areas in the GMT+200 timezone
- Some of the comments in the Android malware are in Hindi: Suggests ties to India
- Some text strings in the BlackBerry malware are Arabic: Suggests ties to the Middle East
- The string “God_Save_The_Queen” was found within the Black Berry malware: Suggests ties to the UK
- The word documents show some resemblance to word documents used by the Red October APT: Suggests ties to Ukraine and/or Russia
- The iOS malware was developed by someone using the account name “JohnClerk”: Suggests ties to the US or UK
- The encryption key for the iOS malware "fjkweyreruu665E62C:GWR34285U^%^#%$%^$RXYEUFQ2H89HCHVERWJFKWEhjvvehhewfD63TDYDGTYEDT23Y" appears to be keyboard mashing on a US/US International keyboard: Suggests ties to the US

Attacks Expanded to Target Mobile Devices

Attackers have expanded their efforts to include malware for Android, BlackBerry and iOS devices.

These are used to gather information from the victims, including phone call recordings. Specifically on the Android platform, they are recording incoming and outgoing phone calls to MP4 sound files that are periodically uploaded to the attackers.

In parallel, there are indications of a large scale MMS phishing campaign probably aimed at selected individuals. According to data obtained by Blue Coat researchers, the intended victims may have been customers of many mobile operators – we know over 60 mobile providers affected, but the real number is likely far higher. The MMS phishing messages have been prepared for multiple countries in Asia (including the Russian sphere and China), Africa, Middle East and Europe.

Conclusion

There clearly is a well-resourced and very professional organization behind Inception, with precise targets and intentions that could be widespread and harmful. The complex attack framework shows signs of automation and seasoned programming, and the number of layers used to protect the payload of the attack and to obfuscate the identity of the attackers is extremely advanced, if not paranoid.

Attribution is always hard, and in this case it is exceedingly difficult. Based on the attributes of the attack and the targeting of individuals connected with national political, economic and military interests, the party behind Inception could be a medium-sized nation state, or possibly a resourceful and professional private entity.

The comprehensive infrastructure suggests that this is a large campaign, of which we’ve only seen the beginning. While the majority of the targets seem to be located in Russia or related to Russian interests, there are verified targets in countries all over the world, and the attack could potentially expand globally. In addition, this infrastructure model does not need to be applied solely against a few targets, nor hosted at CloudMe. The framework is generic, and will work as an attack platform for a multitude of purposes with very little modification.

Additional Guidance - What You Can Do

Signs of compromise

- Unauthorized WebDAV traffic
- regsvr32.exe continuously running in the process list

Ways to prevent infection

- Keep software updated
- Don’t jailbreak mobile phones
- Don’t Install apps from unofficial sources

Signs of being targeted

- Unsolicited emails containing rtf documents
- Unsolicited emails or MMS messages suggesting smart phone applications need updating

Get the full report: "The Inception Framework: Cloud-Hosted APT."