Quick Heal

Security Simplified

Advanced Persistent Threat

Annual Report 2015

Executive Summary

This report aims to highlight some of the major Advanced Persistent Threat samples detected by the Quick Heal Threat Research and Response team in 2015. These attacks were analyzed based on their threat level, propagation, behavior post infection, detection statistics, common tactics used by attackers, and C&C (command and control) servers-related information. The analysis revealed that a majority of the targeted companies are Government, Finance, Infrastructure, and Defense organizations. It is also indicated that the most common entry for these attacks are emails and malicious attachments, propagated using spear phishing and social engineering techniques. The same concludes that zero-day threats and security vulnerabilities in the most popular software programs such as Microsoft Office, Adobe Flash, Java and others are the primary entry points for APTs. Further, browser-based exploits are also becoming more prevalent and common for deploying APTs into networks. Recommendations discussed include:

1. Keeping applications and Operating Systems patched and up-to-date
2. Having a contingency plan to deal with APTs
3. Conducting cyber safety awareness training for employees
4. Having an effective vendor management and incident resolution plan

Table of contents

Introduction

A targeted attack a.k.a. Advanced Persistent Threat (APT) is a type of a threat developed to steal confidential and critical data from targeted systems. The purpose of APTs is to steal Intellectual Property or extract confidential information over a period of time, instead of carrying out a short-term but deadlier attack or denial of service. There are various steps involved in APT attacks; they include intelligence-gathering, point of entry, command and control (C&C) server communication, lateral movement and data stealing. APTs have been making headlines globally for a few years now, and it comes as no surprise that a majority of such attacks are commonly state-sponsored or an indication of targeted cyber-espionage attacks.

In 2015, the Quick Heal Threat Research and Response team detected several Advanced Persistent Attacks that were aimed towards Government, Finance, Infrastructure, and Defense sectors. Many of these attacks were targeted toward Indian organizations also. This report presents a brief analysis of all these attacks, their working, detection statistics followed by common tactics used by threat actors and information related to the Command and Control servers related to these attacks.

Attack campaigns/APTs observed in 2015

The below table gives a quick insight into some of the most interesting APTs that were detected by the Quick Heal Threat Research Labs in 2015. The table lists the names of the APTs, their short summary, and the time during which they were detected. The table is followed by a detailed overview of each of these attacks.

APT Name	Brief Description	New Version Detected
APT-QH-4AG15	• Targeted at private sectors and financial organizations. • Uses Anti-VM and Anti-Sandbox techniques to bypass security detection.	August 2015
BNCC	• Targeted at Indian Government Organizations. • Uses malicious MS Office documents (RTF) to exploit the CVE-2012-0158 vulnerability.	February 2015
APT 30	• A 10-year old cyber espionage campaign. • Primary targets include Southeast Asian governments and commercial entities.	April 2015
PlugX	• Targets include various organizations in India. • Was used in attacks against various sectors in Japan in 2012, and Russian telecom and military sectors in 2015.	February 2015
NetTraveler Campaign	• Active since 3 years. • Primary targets are from Mongolia, Russia, and India.	February 2015
Syndicasec	• Also known as WMI Ghost; first reported in 2010. • Has similarities to cyber espionage campaigns targeted at Tibetan activists in the past.	March 2015
Operation India IT News	• Primary targets include Indian Military Organizations. • C&C server identified - 'indiaitnews.info'.	December 2014

TrojanAPT.Agent.150804: Attacks on Financial Organizations

Threat Level: High

Overview: In August 2015, we observed targeted attacks on private sectors and financial organizations. The infection vector is a spam email that comes with an attachment containing a malicious executable file with an appealing name; for example 'fraudulent trns.exe'. Once it is executed by the unsuspecting user, it executes its malicious activities.

The malware takes special care of not executing its payload under the automated analysis systems with Virtual Machines (Anti-VM) and Sandbox (Anti-Sandbox). This attack confirms that advanced threats are loaded with Anti-VM and Anti-Sandbox techniques to bypass analysis under automated detection system.

Propagation: Spear phishing emails.

Behavior post infection: Post infection, the malware gives the attacker full control of the system, allowing them to perform the following activities.

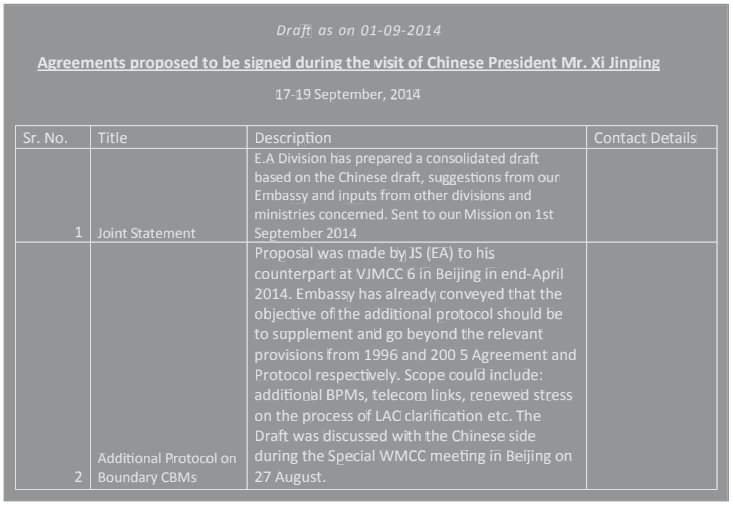
- Steal credentials of Outlook and Live Mail accounts
- Perform keylogging activity
- Take screenshots
- Copy data from clipboard
- Download and execute other malicious components

Further reading: The malware maintains its persistence by copying itself to a startup folder or by making an autorun registry entry. Communication with the C&C server is in plain text and not encrypted. It can send clipboard data and screenshots besides user keylogs. Attackers are using cracked versions of keyloggers like KeyBase, HawkEye Keylogger, and Knight Logger in such campaigns.

TrojanAPT.Agent.150204: Targeted Attacks on Indian Government Organizations

Threat Level: Critical

Overview: The attack uses spear phishing emails with malicious Microsoft Office documents (RTF) as attachments that exploit the CVE-2012-0158 vulnerability. When the user opens this malicious RTF file it drops an executable component on the targeted system. Below is an example of a decoy document used in this attack. The attack uses a RAT tool that includes commands named 'bncc', hence the name for the campaign.



Draft as on 01-09-2014

Agreements proposed to be signed during the visit of Chinese President Mr. Xi Jinping

17-19 September, 2014

Sr. No.	Title	Description	Contact Details
1	Joint Statement	E.A Division has prepared a consolidated draft based on the Chinese draft, suggestions from our Embassy and inputs from other divisions and ministries concerned. Sent to our Mission on 1st September 2014	
2	Additional Protocol on Boundary CBMs	Proposal was made by JS (EA) to his counterpart at VJMCC 6 in Beijing in end-April 2014. Embassy has already conveyed that the objective of the additional protocol should be to supplement and go beyond the relevant provisions from 1996 and 200 5 Agreement and Protocol respectively. Scope could include: additional BPMs, telecom links, renewed stress on the process of LAC clarification etc. The Draft was discussed with the Chinese side during the Special WMCC meeting in Beijing on 27 August.	

Fig. (1) Decoy document

Propagation: Spear phishing emails.

Behavior post infection: The malware is designed to execute the following malicious activities.

- Collect user and system information
- Collect information of the list of running applications of drives
- Search for files with specific extensions

Further reading: The dropped file copies itself to the 'C:\Program Files\Common Files\Microsoft Shared\WindowsUpdate' folder with names 'svc.exe' and 'svchos.exe' making file attribute as hidden. It also drops MS12027_Dll.dll which is used to bypasses the UAC (User Account Control) mechanism in Windows to run arbitrary commands with elevated privileges without showing any prompts to users. The code used is same as demonstrated by Leo Davidson in 2009. The version information of MS12027_DLL.dll shows its language as Chinese (PRC); PRC stands for People's Republic of China. New variants of this dll have no version information.

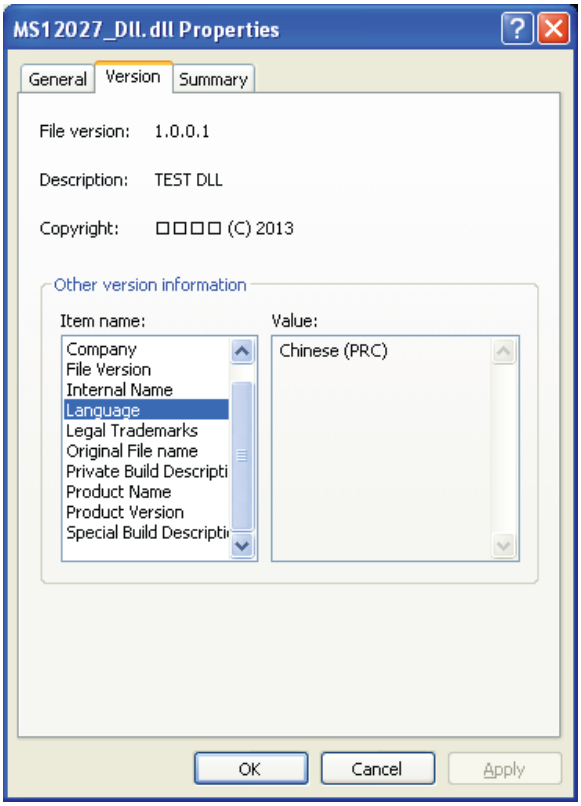


Fig. (2) Version information of MS12027_DLL.dll

svchos.exe file is registered as service 'Windows Service Filter Framework' under this registry key - HKLM\SYSTEM\CurrentControlSet\Services\WCSFilter

It supports the following 5 commands in two modes differentiated with 's' and 'm' parameters:

- -[s|m] -install -bncc
- -[s|m] -uninstall -bncc
- -[s|m] -start -bncc
- -[s|m] -stop -bncc
- -[s|m] -copyto -bncc

The malware creates a list of all files present on the system. '1qaz2345wsxcderd1qaz2345' is used as a key to encrypt compressed CAB file with directory listing. It checks for files with extensions .pptx, .xlsx, .docx,

.ppt, .xls, .pdf, .doc, .txt, and .jpg. It copies these files to the 'System Volumn Information' folder which is then made as a system and read-only folder using desktop.ini trick; it creates desktop.ini in the folder with the following data:

[.ShellClassInfo]
CLSID={645FF040-5081-101B-9F08-00AA002F954E}

TrojanAPT.Agent.150317: APT 30 Cyber Espionage Campaign

Threat Level: Critical

Overview: APT 30 is a highly organized cyber espionage campaign that has been running for more than 10 years now. Its main purpose is stealing data for political gain. The campaign is known to be used for spying on Southeast Asian governments and commercial entities. This campaign uses multiple components like downloader, backdoors, and sophisticated C&C infrastructures. The malware used in that attack infects removable drives to infiltrate air-gapped networks. It is designed to work stealthily and persistently for long durations.

Propagation: Spear phishing emails.

Behavior post infection: The malware used in this attack, performs the following activities:

- Infect removal drives
- Download and execute specified file
- Support functionality to run malware in stealth mode or run mode
- Get list of hostnames to perform version check for self-update
- Get stage 2 C&C server list

Further reading: This is a case of state-sponsored cyber espionage with multiple teams involved in it. The different malware tools used in it are known as 'Backspace', 'NetEagle', 'ShipShape', 'SpaceShip' and 'FlashFlood'. Communication of the malware with the C&C server goes through filtering of two stages at server side.

Major political events are systematically used for designing social engineering attacks to target individuals in diplomatic and leadership roles. Some of these targets include personnel from Indian Defense and Telecommunication organizations.

Quick Heal Threat Research Labs has received many samples related to this campaign. Detections for them have increased from 6,000 to 15,000 in Q4-2015.

TrojanAPT.Agent.150209: PlugX

Propagation: Critical

Overview: This campaign was first observed in February 2015 against

certain organizations in India. It used spear phishing emails with malicious Microsoft Office (RTF) documents as an attachment that exploited the CVE-2012-0158 vulnerability. When a user opens the malicious RTF file, it drops a decoy document and executable with a random name in the %temp% folder.

Propagation: Spear phishing emails.

Behavior post infection: Using the malware, the attacker can accomplish the following:

- Keylogging
- Screen capturing
- Remote desktop access
- Executing specified SQL statements
- Controlling the lock-unlock shutdown and rebooting of a machine
- Enumerating processes and drives

Further reading: PlugX uses DLL Side-Loading technique to load its malicious payload into the signed executable 'fsguidll.exe', an F-Secure GUI Component. The payload is decompressed and injected into the system processes - svchost.exe and explorer.exe which remains in the process memory and never stored on disk. To remain persistent in its attack, fsguidll.exe registers itself as a service with a random name. The C&C server in this case was unisers.com which resolves to 203.XXX.232.XXX, hosted in Hong Kong.

Similar attacks using PlugX were also observed against various sectors in Japan back in 2012, and Russian telecom and military organizations in July 2015.

TrojanAPT.Agent.150205: NetTraveler Campaign

Threat Level: Critical

Overview: This is one of the most consistent APT campaigns. It has been running for more than 3 years now, attacking victims in various countries like Mongolia, Russia, and India. The attack uses spear phishing emails with malicious RTF attachments that also exploit the CVE-2012-0158 vulnerability. When a user opens the malicious RTF file, it drops a malicious executable. It creates an LNK file under %Startup% folder to execute its main payload component or registers a service named 'Net Security Service' to remain persistent in the victim's system.

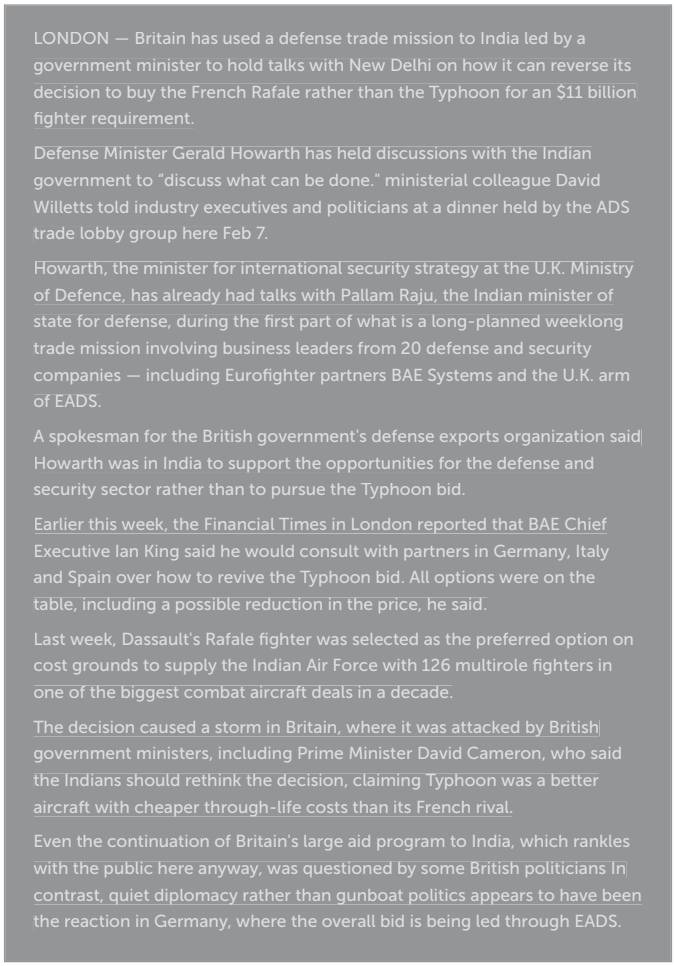
Propagation: Spear phishing emails.

Behavior post infection: The malware is designed to perform the following activities:

- Gather the infected system's details
- Download and execute new malicious components from the C&C server

Further reading: Several of the decoy documents used in this attack, indicate

that victims of this campaign were Indian Government organizations.



LONDON — Britain has used a defense trade mission to India led by a government minister to hold talks with New Delhi on how it can reverse its decision to buy the French Rafale rather than the Typhoon for an $11 billion fighter requirement.

Defense Minister Gerald Howarth has held discussions with the Indian government to "discuss what can be done." ministerial colleague David Willetts told industry executives and politicians at a dinner held by the ADS trade lobby group here Feb 7.

Howarth, the minister for international security strategy at the U.K. Ministry of Defence, has already had talks with Pallam Raju, the Indian minister of state for defense, during the first part of what is a long-planned weeklong trade mission involving business leaders from 20 defense and security companies — including Eurofighter partners BAE Systems and the U.K. arm of EADS.

A spokesman for the British government's defense exports organization said Howarth was in India to support the opportunities for the defense and security sector rather than to pursue the Typhoon bid.

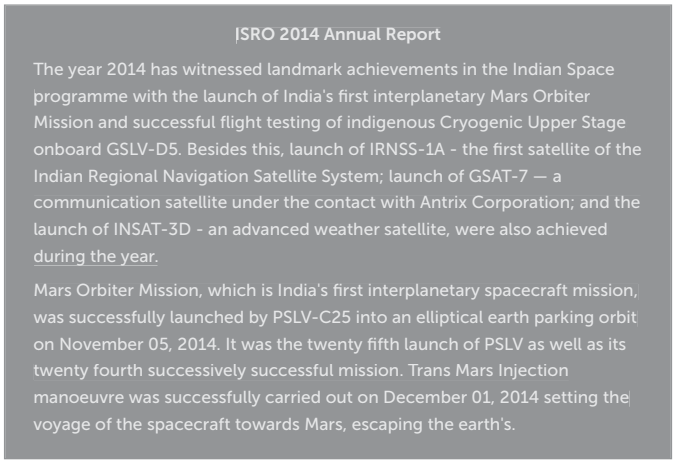
Earlier this week, the Financial Times in London reported that BAE Chief Executive Ian King said he would consult with partners in Germany, Italy and Spain over how to revive the Typhoon bid. All options were on the table, including a possible reduction in the price, he said.

Last week, Dassault's Rafale fighter was selected as the preferred option on cost grounds to supply the Indian Air Force with 126 multirole fighters in one of the biggest combat aircraft deals in a decade.

The decision caused a storm in Britain, where it was attacked by British government ministers, including Prime Minister David Cameron, who said the Indians should rethink the decision, claiming Typhoon was a better aircraft with cheaper through-life costs than its French rival.

Even the continuation of Britain's large aid program to India, which rankles with the public here anyway, was questioned by some British politicians In contrast, quiet diplomacy rather than gunboat politics appears to have been the reaction in Germany, where the overall bid is being led through EADS.

Fig. (3) Decoy document



ISRO 2014 Annual Report

The year 2014 has witnessed landmark achievements in the Indian Space programme with the launch of India's first interplanetary Mars Orbiter Mission and successful flight testing of indigenous Cryogenic Upper Stage onboard GSLV-D5. Besides this, launch of IRNSS-1A - the first satellite of the Indian Regional Navigation Satellite System; launch of GSAT-7 — a communication satellite under the contact with Antrix Corporation; and the launch of INSAT-3D - an advanced weather satellite, were also achieved during the year.

Mars Orbiter Mission, which is India's first interplanetary spacecraft mission, was successfully launched by PSLV-C25 into an elliptical earth parking orbit on November 05, 2014. It was the twenty fifth launch of PSLV as well as its twenty fourth successively successful mission. Trans Mars Injection manoeuvre was successfully carried out on December 01, 2014 setting the voyage of the spacecraft towards Mars, escaping the earth's.

Fig. (4) Decoy document

The malware opens a backdoor and connects to the following C&C server and passes the infected machine's information details as shown below:

<C&C Server Name>/<Client Request ID><Encrypted Volume Serial No><Computer Name><User Name>

C&C server used are as below:

C&C server	IP Address	Location
godson355.vicp.cc	174.XXX.255.XXX	United States
www.indiacertpsed.com	203.XXX.232.XXX	Hong Kong
unisers.com	203.XXX.232.XXX	Hong Kong
pstestnew.minidns.net	61.XXX.4.XXX	China
worldeyesinter.com	95.XXX.172.XXX	Netherlands

TrojanAPT.Agent.150324: Syndicasec - New version of Syndicasec with rootkit technique

hreat Level: High

Overview: The first version of Syndicasec a.k.a. 'WMI Ghost' was reported back in 2010. It was used in different campaigns by various groups for years and is still being reported in the wild. In March 2015, a new variant of Syndicasec was detected by Quick Heal Threat Research Labs. In its previous avatar, it was using WMI Registered JavaScript which is now executed as a native code. Attackers have added kernel mode driver 'amd32.sys' to hide user mode payload process. The entry vector here again is a malicious RTF document with CVE-2012-0158 in a spear phishing mail.

Propagation: Spear phishing emails.

Behavior post infection: The malware allows an attacker to carry out these activities:

- Download files from specified URLs
- Encrypt specified files with XOR encryption algorithm and upload it to C&C server
- Executing specified files

Further reading: A hardcoded Stage 1 C&C server points to a fake RSS blog containing encrypted strings for Stage 2 C&C servers. The delimiter is changed from '@' to '@@' in the new version, with more complex encryption and obfuscation.

Few of the examples of Stage 1 C&C servers from the analyzed samples are:

- adoorbha[removed]ess.com/feed/
- andy5698[removed]nal.com/data/rss
- blogs.re[removed]anilchopra/feed/
- blogs.re[removed]arunachali/feed/
- blogs.re[removed]bhishma/feed/
- blogs.re[removed]kellysblog/feed/
- blogs.re[removed]yescomeon/feed/
- fastlist[removed]dns.com/A/feed.xml
- hi.baidu[removed]k2012/rss
- jstarted[removed]/feed/
- jstarted[removed]com/rss.xml
- jstarted[removed]s.com/feed/
- umar809[removed]rnal.com/data/rss

Examples of Stage 2 C&C servers:

- owner.102.[removed]pian.com/l3/l3.php
- sportnews.[removed]oool.com/S/index.php
- www.eadtra[removed]com/zy/proxy.php
- www.pattan[removed]raju.org/123/hello.php

This operation has similarities to cyber espionage campaigns used against Tibetan activists in the past.

MAHANAGAR TELEPHONE NIGAM LLMITED
(A Government of India Enterprise)
CORPORATE OFFICE
HR BRANCH
Jeevan Bharati, Tower-I, 12th Floor, 124, Connaught Circus, New Delhi 110 001

PUBLISHED BY HR SECTION OF MTNL CORPORATE OFFICE

MTNL Senior Management Services' Promotion Policy

No. MTNL/CO/R & E/2009 Dated:10.03.2015 at New Delhi

1. **SHORT TITLE AND COMMENCEMENT:** With the approval of MTNL Board, the following rules relating to recruitment of Executives in MTNL are hereby made:

Fig. (5) Decoy document

TrojanAPT.Agent.141210: Operation 'India IT News'

Threat Level: Critical

Overview: This is one of most prevalent targeted attacks against Indian Military organizations. Consistent detections were observed Q1-2015. The attack is launched using a Microsoft Office Excel Document with an alluring name, for example, 'Army_Welfare_Housing_Organization_?Defence_Forces_Personnel_plot_scheme.xls'. This contains a Visual Basic Macro which downloads and executes the downloader from the C&C server when opened. The downloader further downloads a dropper which extracts and drops other subcomponents as shown below in Fig. (6).

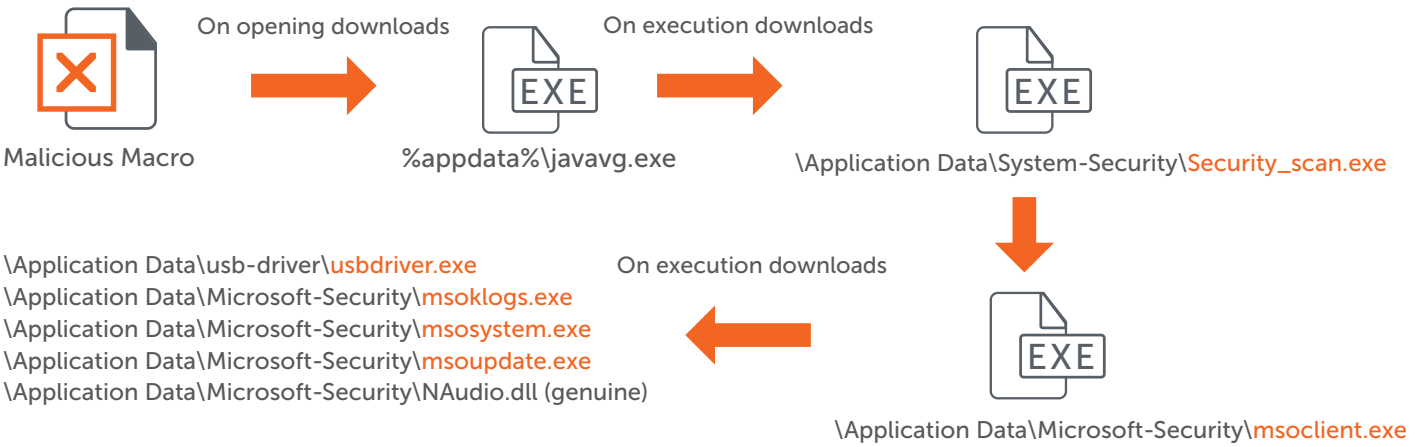


Fig. (6) Execution stages

Propagation: Spear phishing emails.

Behavior post infection: The C&C server identified in this case was 'indiaitnews.info', resembling to 'indiaitnews.com' which is a clean website.

- msoclient.exe communicates with the C&C server and supports extensive commands for surveillance, file operations, process management, and data exfiltration.
- msosystem.exe supports a functionality to steal stored password from web browsers - Internet Explorer, Chrome, and Firefox.
- msoklogs.exe is a keylogger component that saves typed keys and active window names in the app-data%\Microsoft-Security\mslogs file in plain text.
- usbdriver.exe continuously monitors USB drives connected to the infected system for important document extensions like pdf, doc, docx, xls, xlsx, ppt, pptx, pps, ppsx, and txt. These files are copied to '%app-data%\usb-driver\data' folder to be sent to the C&C server later.
- msoupdate.exe acts kill bit to clean all the components and folder created after successful data exfiltration.

Further reading: Based on file information, it could be seen that this project was started between October and November 2014. It was at its peak - accounting to more than 50000 detections in Q1 2015 (Please refer to Fig. 7 - Detection Statistics)

The targets include Indian Military personnel, people related to Indian Politics, top management officers from private companies and even celebrities.

Remote Access Trojan (RAT) functionality

As discussed above, these threats are fully equipped with RAT functionalities that are required for cyber espionages:

- Steal user information like username, hostname and Operating System version
- Listing all drives
- Enumerating of files on all drives
- Enumerating running processes
- Terminating specific processes
- Downloading file from specified links
- Executing specified file
- Uploading files to remote server
- Enumerating active windows
- Taking desktop snapshots
- Keylogging
- Stealing saved login credentials from email clients, web browsers and FTP Clients, etc.

Detection Statistics

The below figure highlights the statistics of the major APTs detected in 2015.

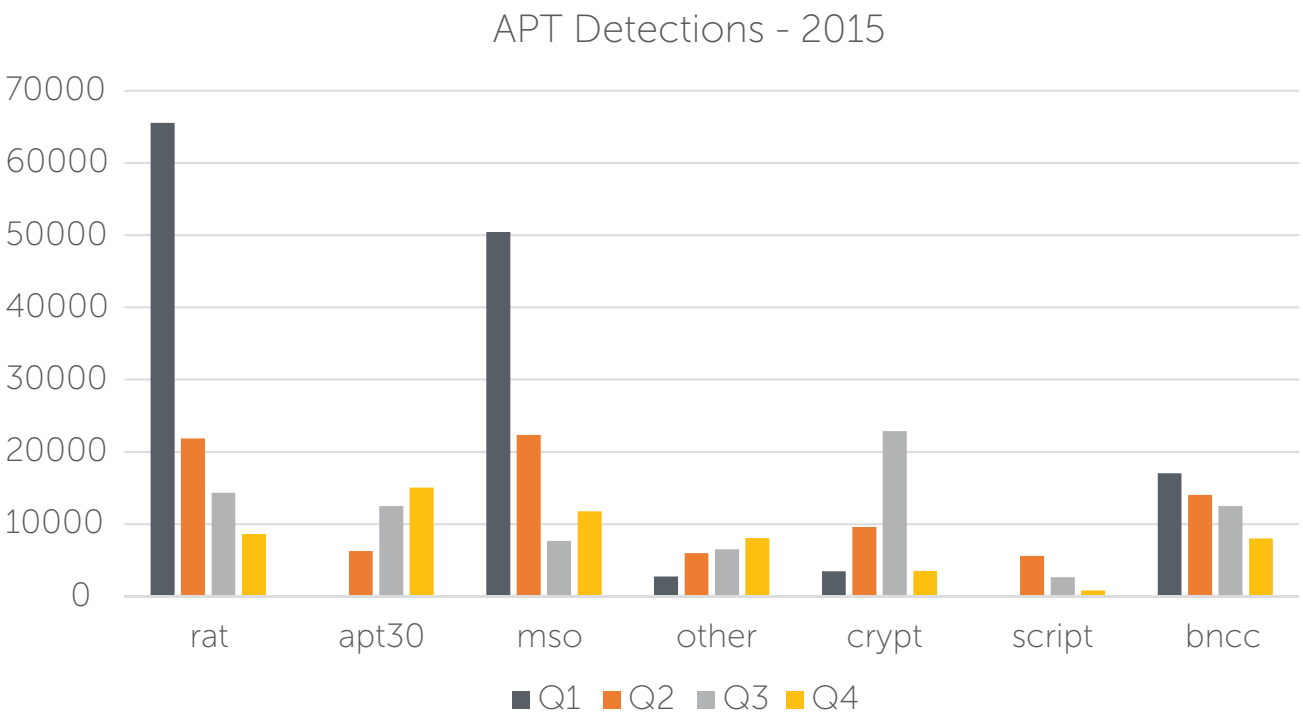


Fig. (7) APT Detections - 2015

Definitions:

rat – Remote Access Tools (e.g. Poison Ivy) detections
apt30 – APT 30 campaign
mso – components used in the Operation India IT News
other – remaining APT detections
crypt – cryptors used for delivery of APT
script – APTs using AutoIT, Javascript, and ZXShell
bncc – components of bncc attack

Major Trends

Known vulnerabilities are used as systems remain unpatched

Security vulnerabilities reported and fixed more than 3 years ago are still being used by attackers. For example, HTML (CVE-2010-0806), RTF (CVE-2012-0158, CVE-2014-1761), Java (CVE-2012-0507), and Microsoft Office (CVE-2014-6352) are still exploited persistently in the wild and for targeted attacks.

Threats are heavily loaded with Anti-Sandbox, Anti-VM and Anti-Emulation Techniques

Recent APT samples indicate heavy use of anti-sandbox, anti-VM and anti-emulation techniques that either stop or delay execution of malicious behaviors when running under automated analysis systems. This aids the malware to bypass security detection.

Use of social media sites and domain names that avoid user suspicion

Attackers are increasingly using domain names that resemble commonly used news, social media or government sites. C&C server information is kept on blog hosting sites in encrypted form. This methodology helps attackers to avoid suspicion by users and IT Security professionals. Below are some examples of names used for C&C servers:

- indiacertpsed.com
- gov.erpds.com
- india.wikaba.com
- indiaitnews.info
- india-time.org

Usage of scripting languages like AutoIT, Python and Javascript

As scripts run as part of trusted process, they are most likely to be ignored by behavior-based detection systems. These scripts are obfuscated so that they remain undetectable for a longer period of time. Detection statistics shows over 10,000 detections for components using AutoIT and Javascript in 2015.

Remote Access Tools (RAT) or system tools are used for stealing stored passwords and data exfiltration

Poison ivy - Poison ivy RAT is a popular tool among cyber attackers - accounting for more than 1,10,000 detections in 2015. It provides an easy way to create a RAT tool with surveillance functionalities such as keylogging, screen capturing and stealing Windows stored passwords. Web browsers and email client password recovery tools from Security Xploded and Nirsoft are used in some of these campaigns. Quick Heal detects all such tools as Hack-tools.

Future Predictions

1. Spear phishing and social engineering techniques will continue to exploit known and zero-day vulnerabilities to deliver sophisticated payloads.
2. Complex encryption and obfuscation techniques will constantly evolve to evade detection by security products. The usage of cryptors is seen to increase by each quarter.
3. Attackers will avoid saving executable components on disk by having them in an encrypted form and decrypting it runtime in the process memory.
4. Attackers will continue to innovate and add more Anti-Sandbox and Anti-VM techniques to bypass detection and automated analysis by Sandboxing. In recent months, researchers have targeted and demonstrated vulnerabilities in Sandbox solutions and Network-based security products that could provide remote code execution and backdoor. This opens a greater attack surface for attackers to gain entry into organizations armed with super remote access.

Conclusion

Going forward, there are several trends that security solution vendors and enterprise network owners need to be wary about. Zero-day threats and security vulnerabilities in the most popular software programs such as Adobe Flash, Java and more are the primary entry points for the APTs that we have detected over the last few months. It is crucial for network administrators to be aware of these threats and ensure that their operating systems and applications are always updated to the latest patches and versions. Leaving security holes open due to unpatched software in this day and age is as good as leaving the backdoor open. Browser-based exploits are also becoming more prevalent and common for deploying APTs into networks, so effective layers of security solutions are needed.

Enterprises also need to accept the possibility that their systems can be compromised by APTs at any time. Facilitating a plan of action and a contingency scenario for such situations is now an essential component of IT strategies. Awareness training, effective vendor management and incident resolution plans are recommended steps for protecting the sensitive information within organizations.

A certain gap also exists in the market between understanding what an APT does and what it actually is. Closing this gap can only be achieved with proper compliance policies and technical training at the right places. Mechanisms that are built for protection against standard viruses and malware threats will not be effective against highly targeted and difficult-to-detect APTs. New technologies that are designed to detect and combat APTs specifically need to be widely adopted and put into place, no matter how high the investment. At the end of the day, customized attacks such as APTs need customized detection and security solutions to combat them.

To learn more, visit us at www.quickheal.com | www.seqrite.com

ACKNOWEDGMENTS

1. **Subject Matter Experts**
   Prakash Galande
   Sagar Daundkar
   Sudhanshu Dubey
2. **Threat Research & Response Team, Quick Heal**