Threat Report 2017-18

REVE antivirus

www.reveantivirus.com

CONTENTS

Introduction:

REVE Antivirus was started in the year 2014 as an entity of 'The REVE Group'. Within a short span of time, REVE Antivirus has been able to create quality security products for Windows and mobile platform.

We perform extensive R & D that facilitates us to develop home & enterprise level security solution that helps user remain one step ahead of cyber threats.

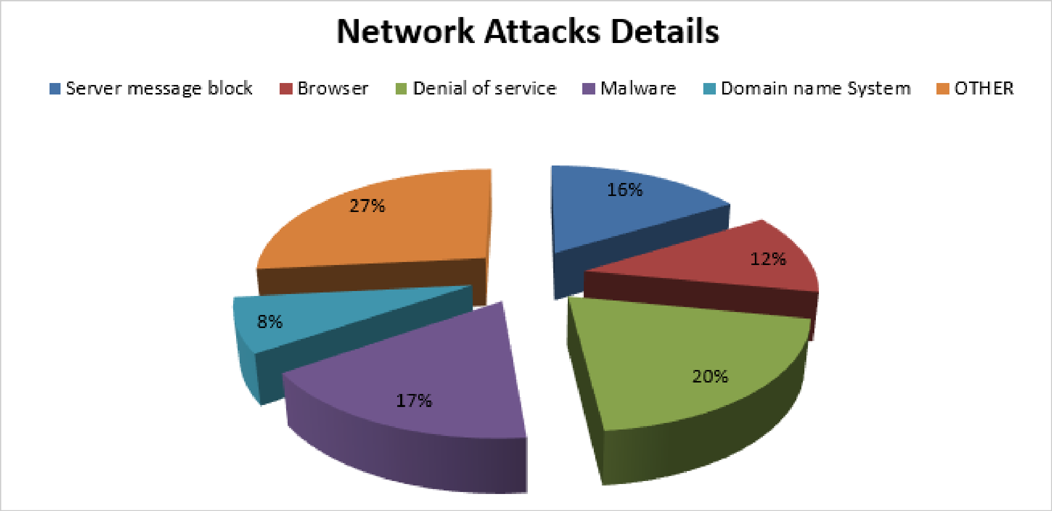
The following report has been created after extensive analysis of the recent malware attacks.

OBJECTIVE:

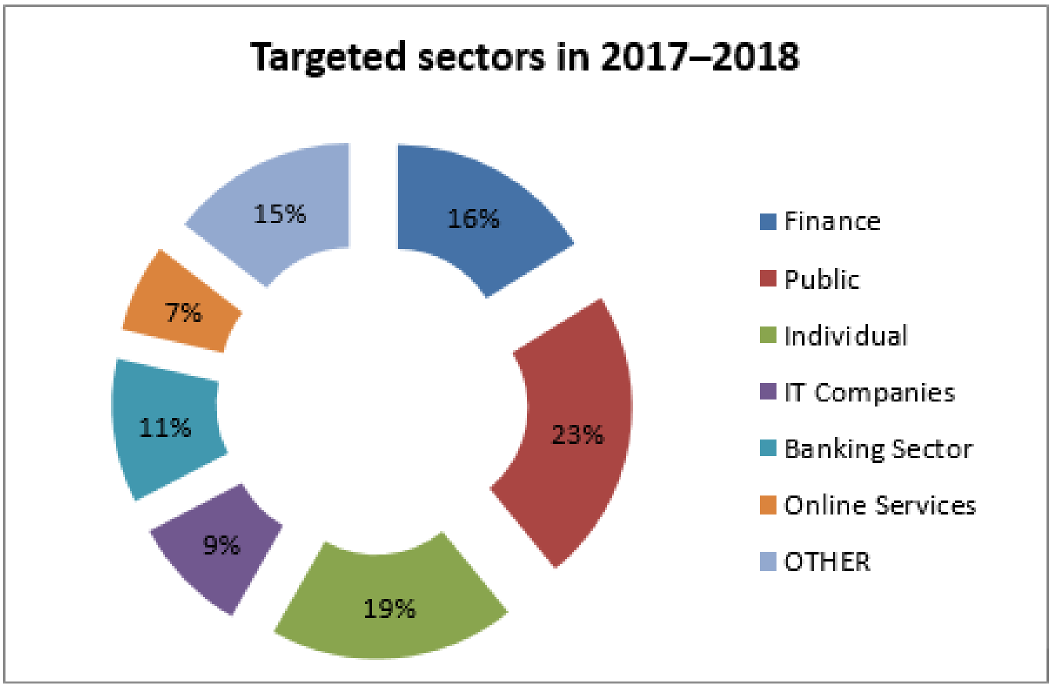
This Report focuses on the latest malware trends observed, detected and reported by REVE Antivirus. The goal of this threat report is to give subjective bits of knowledge of cyber threats that affected Individual and organizations in 2017. With this report, we aim to ease IT security management for home users, small businesses, and corporate houses.

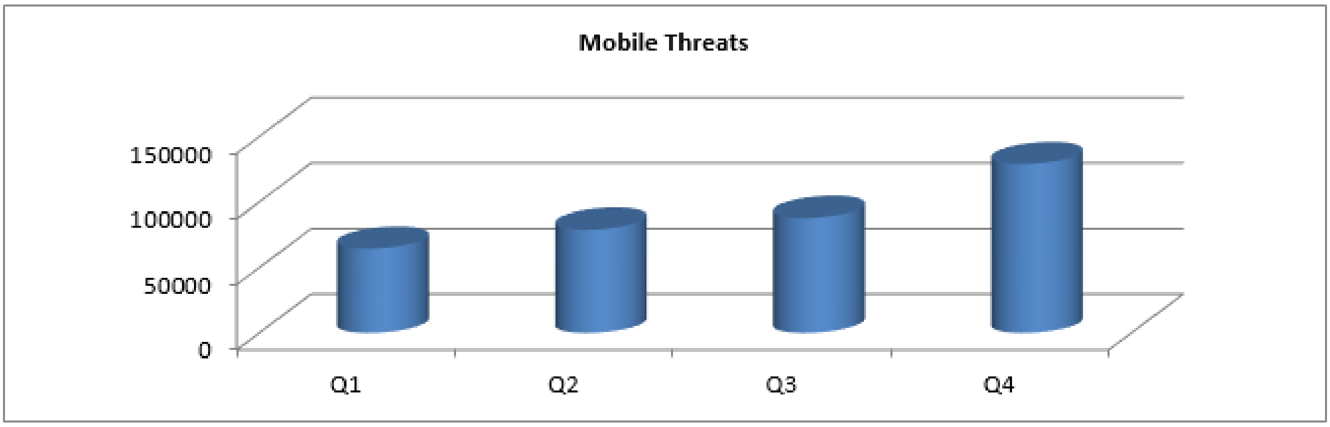
Malware Detection Statistics:

REVE Threat Research enables us to see and dissect real-world assault designs that prompt better customer assurance. Our clients saw the accompanying attack volumes:

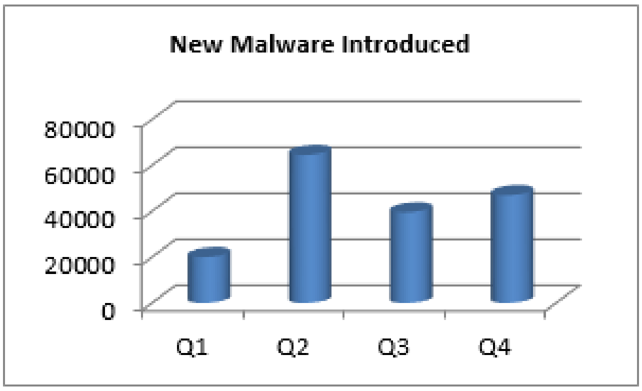


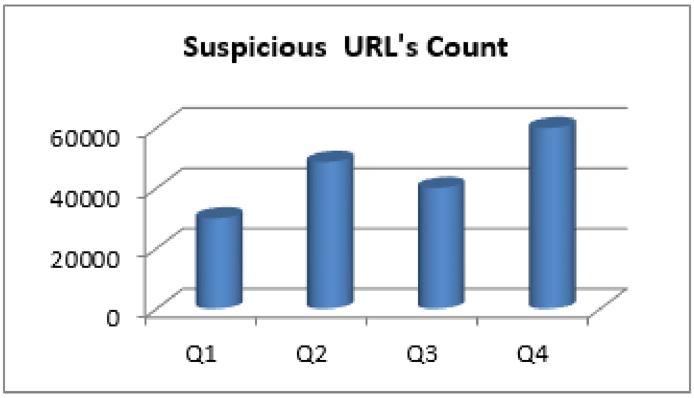
The DDos and Ransomware had significant influence in 2017-18. Banking Sector and individual attacks contributed its major part.





We expect mobile devices to be focused by cyber-criminals in 2018 to launch attacks. Many new malware has been launched and the URL's count has increased.





Top Malware Threats of 2017-18:

1. illicit Bitcoin miners

This is an insidious form of malware consists of a legitimate miner configured to hijack mining efforts to various wallets. The application, along with its configuration file, is clandestinely planted on victims' computers. The definitive way to detect illicit Bitcoin mining operations is by tracking power usage and miners by inspecting network traffic.

2. JS:Trojan.Cryxos

This detection deals with JavaScript code appended to hacked websites to display alarming popups. These Trojans are part of "call or tech support" scams, where compromised websites also display a support number hosting cyber-criminals who offer assistance for a fee.

3. Kovter Malware

Kovter is a Trojan, which was first detected in 2015 and now is back with new techniques. It is spread via email attachments containing malicious office macros compressed by Zip. Kovter is fileless malware that evades detection by hiding in registry keys.

4. Emotet

Emotet is a banking Trojan, designed for stealing banking information, email accounts and automatically withdraw money from victims' bank accounts.
Emotet hijacks infected machines and uses them to spread itself across infected networks, utilizes scheduled tasks and registry entries to spawn copies of itself.

5. Trojan.LNK.

This detection deals with multiple families of malware that use maliciously modified shortcut files with a .LNK extension that are designed to trick users into mistakenly launching a malicious file.

6. Downadup Worm

This is still active on unpatched computers. For nearly 10 years the Downadup worm has been a constant presence in the top threats, beginning with its emergence in 2008. It continues to spread and creates scheduled tasks on infected computers.

7. JS:AdwareJS.Agent

These are introduced through attachments, documents downloaded by user. Once the user downloads the attached file and runs it, the file starts corrupting the system.

WARNING
Virus Detected
To Remove Virus Call Tech Support
Protect Your Personal Financial Information!!
Security Risk
13:24

Looking Ahead to 2018

Ransomware will turn out to be more awful.

The earnestness and the repeat — of cyberattacks achieve a level that nobody could've anticipated. In 2017, WannaCry, NotPetya and Locky, commanded the news cycle as programmers could target organizations universally and cost them billions of dollars. Most ransomware attackers ask to deliver in cryptographic money like Bitcoins whose esteem have as of late begun achieving its pinnacle – a kind of consolation for digital criminals to work harder on their ransomware business. Every year, we think the biggest attacks will go unmatched, but we know that a secure future is the only way to prevent cybercrimes from having a bigger and bolder impact.

IoT will remain a simple picking for attackers

As an ever increasing number of gadgets and open foundation ends up association with the web, and the potential pool for hacks develops exponentially, we'll see more assaults against them. IoT-associated gadgets are more defenseless against attacks, and have just been misused for use in botnets, yet we foresee that they will be focused for regularly in ransomware assaults. We as of now observed the WannaCry ransomware influence little utilities and assembling locales in the United States. In 2018, we'll begin seeing bigger scale attacks against framework and IoT security. The expanded utilization of IoT in the human services industry will likewise make information security worries in 2018

Increase threats to mobile devices

A decade ago, mobile malware was considered a new and unlikely threat. Numerous mobile device clients even viewed themselves as resistant from such dangers. Today, mobile devices are coming under increasing attack and no one is immune. Most of the android apps have become vulnerable to attackers. The multiplication of fake applications and downloading of applications from 3rd party stores were the greatest mobile security concerns. While Apple and Android have made progress in making more secure and hearty working frameworks, pernicious on-screen characters keep on pumping out new and trickier malware

CONCLUSION:-

Our self-satisfied disposition towards cybersecurity is one of the significant reasons why cybercriminals show signs of improvement. We should invest both time and money in securing devices which will ensure our safety from cyber-attacks.