FireEye

Security Reimagined

Regional Advanced Cyber Threat Report
Europe, Middle East & Africa 1H2015

Ray Kafity – VP FireEye Middle East, Turkey & Africa

Table of contents

- Executive Summary
- Crimeware Trend
- Top Crimeware Trend – Dridex/Cridex
- Country Analysis
- APT Malware Families
- Vertical Analysis
  - Government
  - Financial Services
  - Aerospace/Defense

Executive Summary

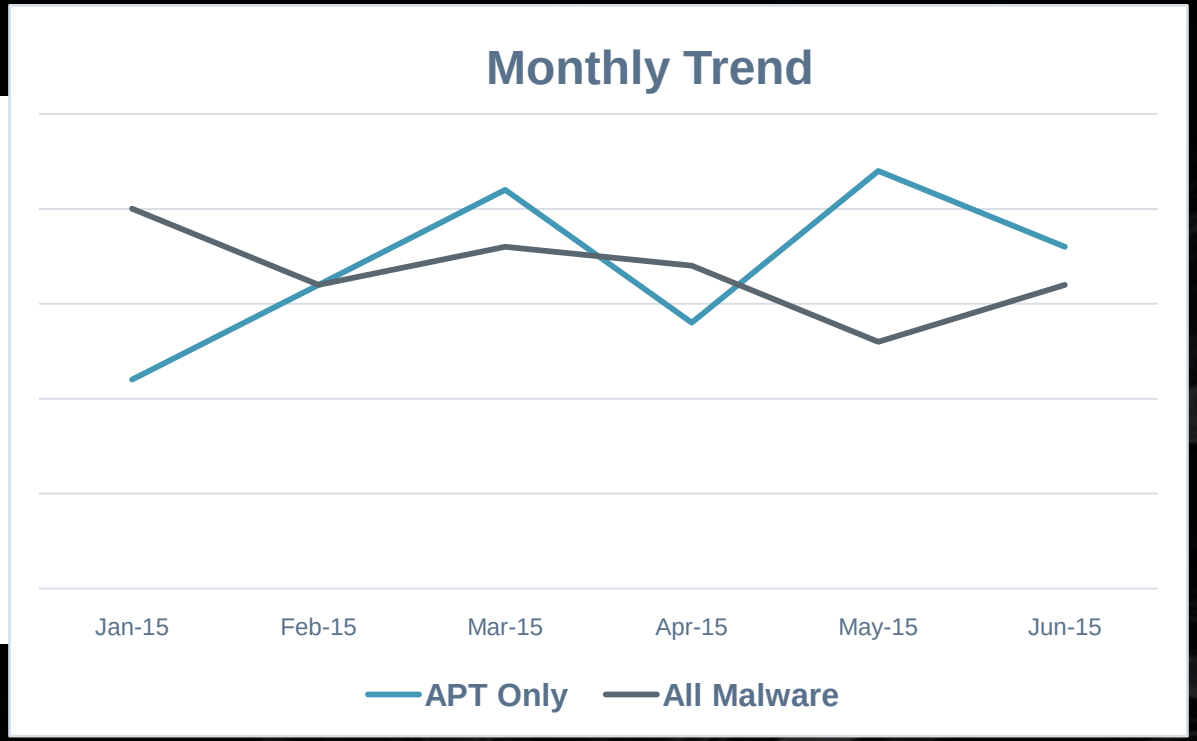
- FireEye Advanced Threat Report for Europe, Middle East & Africa overview of the APT targeting computer networks that were discovered by FireEye during half of 2015 (June 30th, 2015)

- Cyber threat actors are evolving rapidly the level of sophistication to
  - Steal Personal Data & business strategies
  - Gain competitive advantage
  - Degrade operational reliability

Executive Summary

- Report shows:
  - Blurring of the lines – Different cyber threat actors sharing tools, techniques and procedures that lead to numerous and updated indicators of compromise threats.
  - Israel, Saudi Arabia , Spain, UK & Germany are the most targeted countries
  - Energy, Oil & Gas, Government, Aerospace were the most targeted verticals.

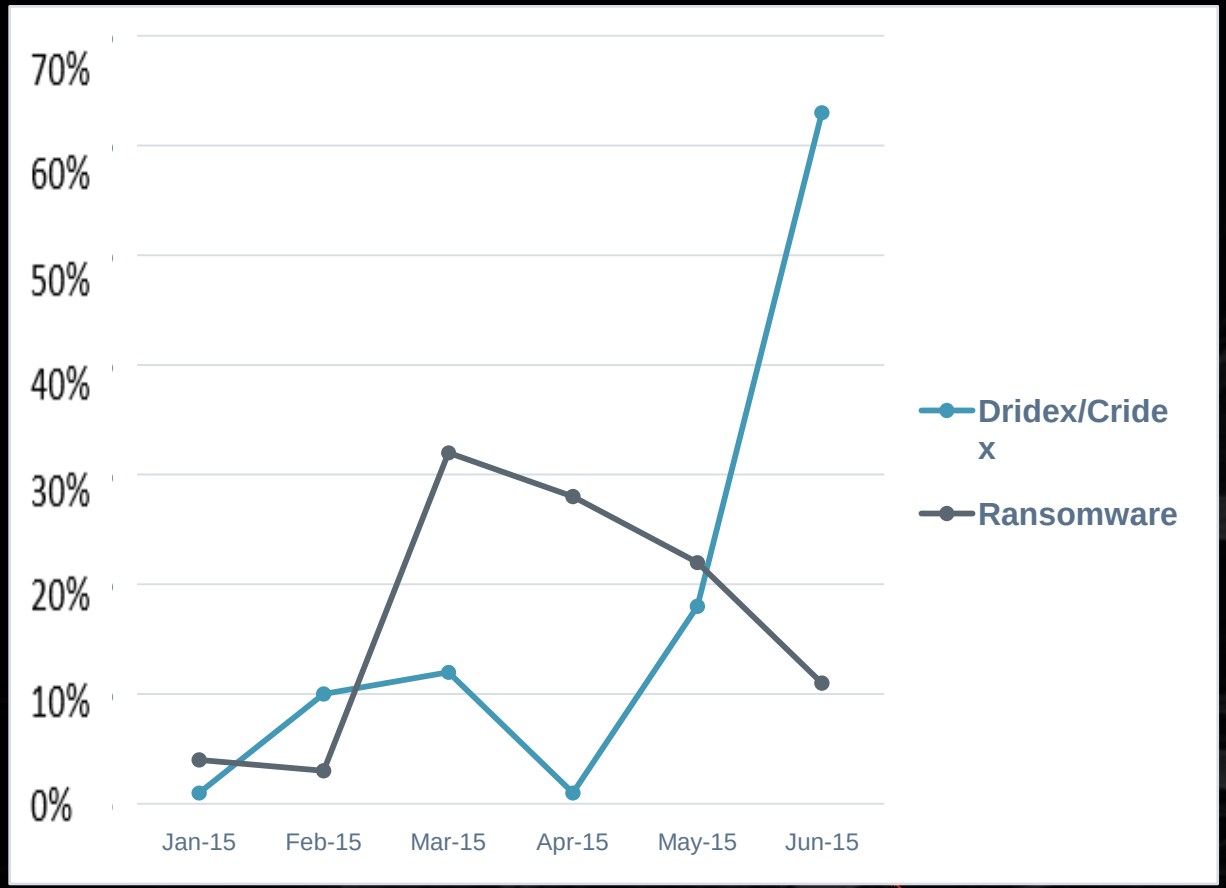
Crimeware Trend



- The number of unique infections has been growing steadily in EMEA.
- The number of crimeware attacks has been steady month after month demonstrating the persistency of cyber criminal threat actors.

FireEye

Crimeware Trend



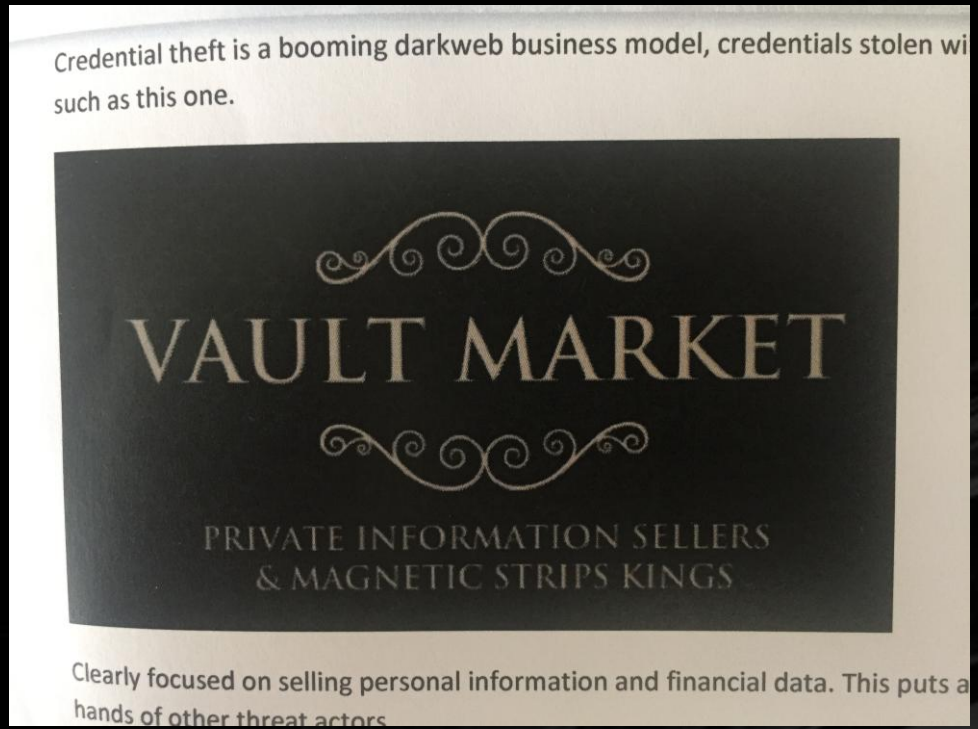
- The graph show the trend of 2 popular crimeware campaigns:
  - Dridex/Cridex.
  - Ransomware
- Dridex/Cridex have considerably grown over time.
- Ransomware going down month after month.
- 60% of Dridex/Cridex unique infections in June 2015.
- Cybercriminals are adapting very rapidly to the new tools, techniques & procedures

FireEye

Top Crimeware Trend – Dridex/Cridex

- Dridex is the new variant of the malware previously known as Cridex/Emotet, Feodo or Bugat that are credential theft trojans.
- Mainly Targeting financial institutions websites but threat actors can configure to capture data from submission to webmail, social networks or file sharing sites.
- Malware distribution through spam emails containing a malicious XLS or DOC attachment.
- Macro in the attachment file that instructs the compromised system to download a malicious executable.
- Communication with the command and control (C2) servers.
- Invoke the use of macros utilizing social engineering methods (pop up boxes)

Top Crimeware Trend – Dridex/Cridex



- Credential theft is a booming business model. Credentials stolen will often end upon darkweb markets such as Vault Market.
- Vault Market is focused on selling personal information and financial data which put them in the hands of other cyber threat actors.

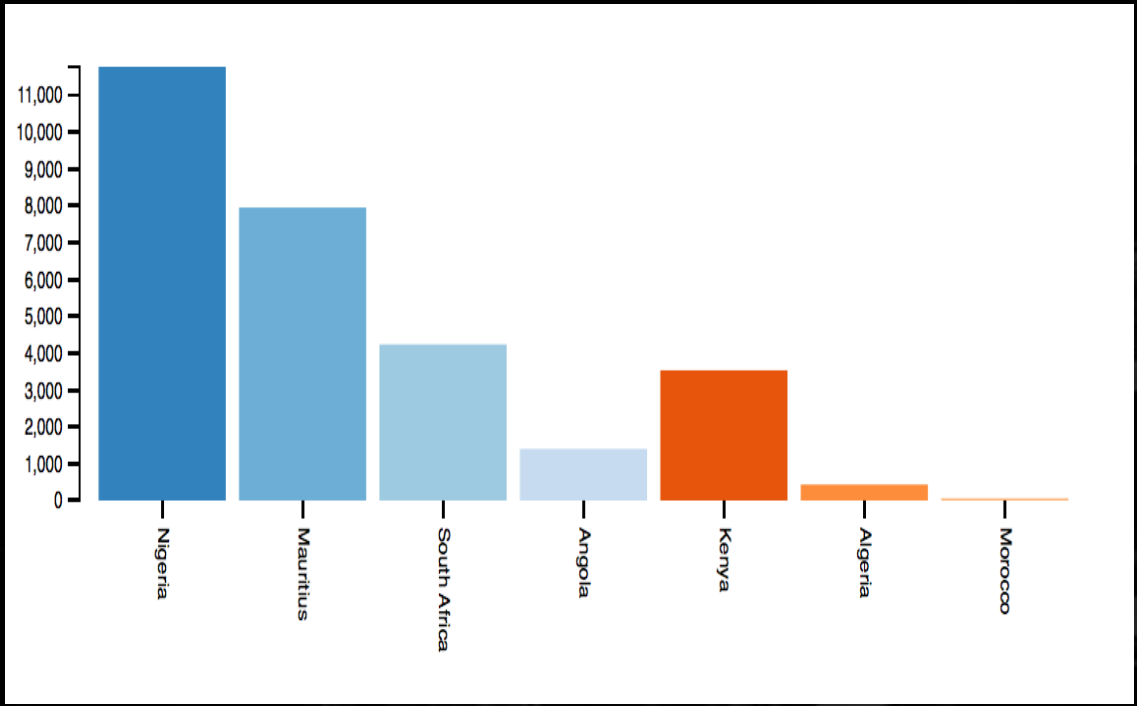
FireEye

Country Analysis

The highest number of APT malware detected in EMEA 1H 2015:

- Israel (11%)
- Saudi Arabia (11%)
- Spain (10%)
- Germany (10%)
- United Kingdom (9%)
- Italy (9%)
- Denmark (6%)
- Turkey (6%)
- Norway (5%)
- Russia (5%)

Africa Report – Across 6 Countries



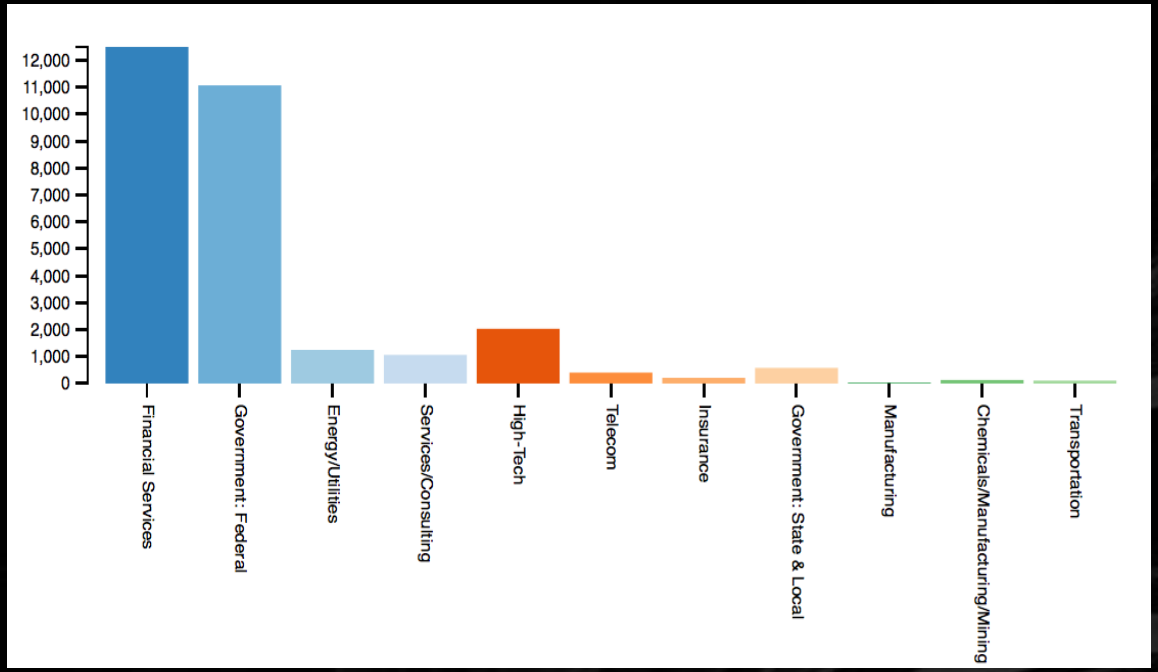
5107 Average no of confirmed Call Backs to CnC Servers across 30 customers

South African & Nigerian Financial Institutions under attack Mauritius Cyber risk at Government Level

Kenya more cyber aware yet System lack as mainly alert drive technologies deployed

FireEye

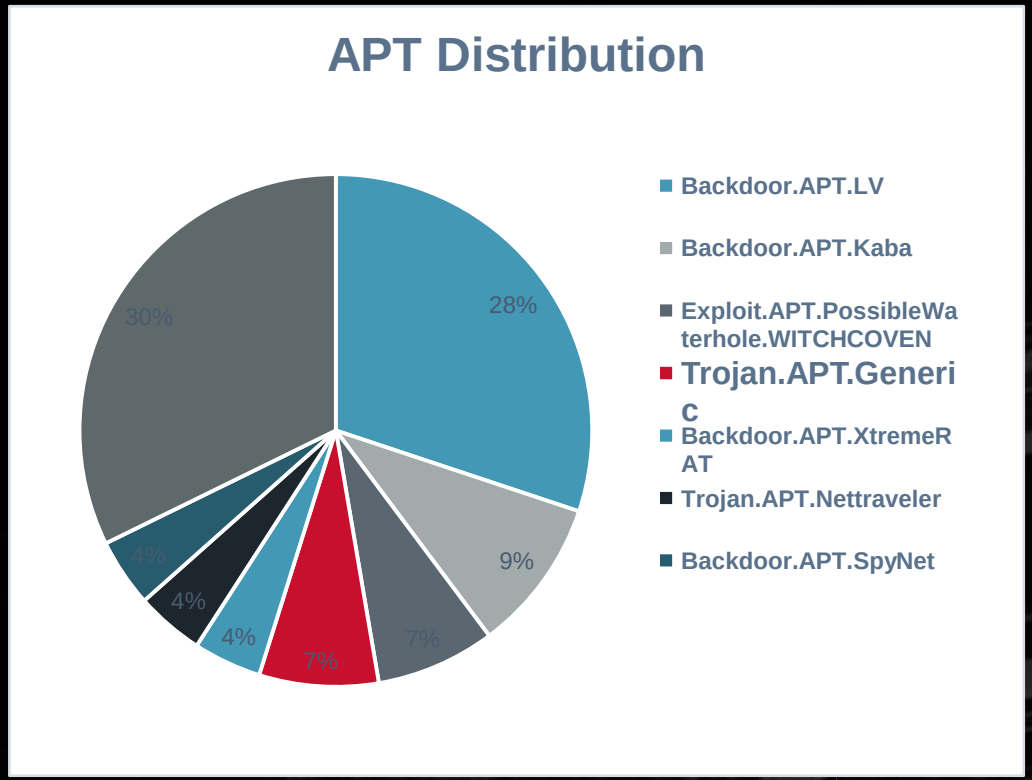
Africa Report – Across 30 Customers



- Financial Institutions & Government most targeted sector
- Threat tactics mapped to Russian & Chinese Threat Actors
- APT 28 Group active in Financial Sector
- Telco Industry data “light” as only 3 telco’s evaluated – evidence suggests this sector is highly targeted

FireEye

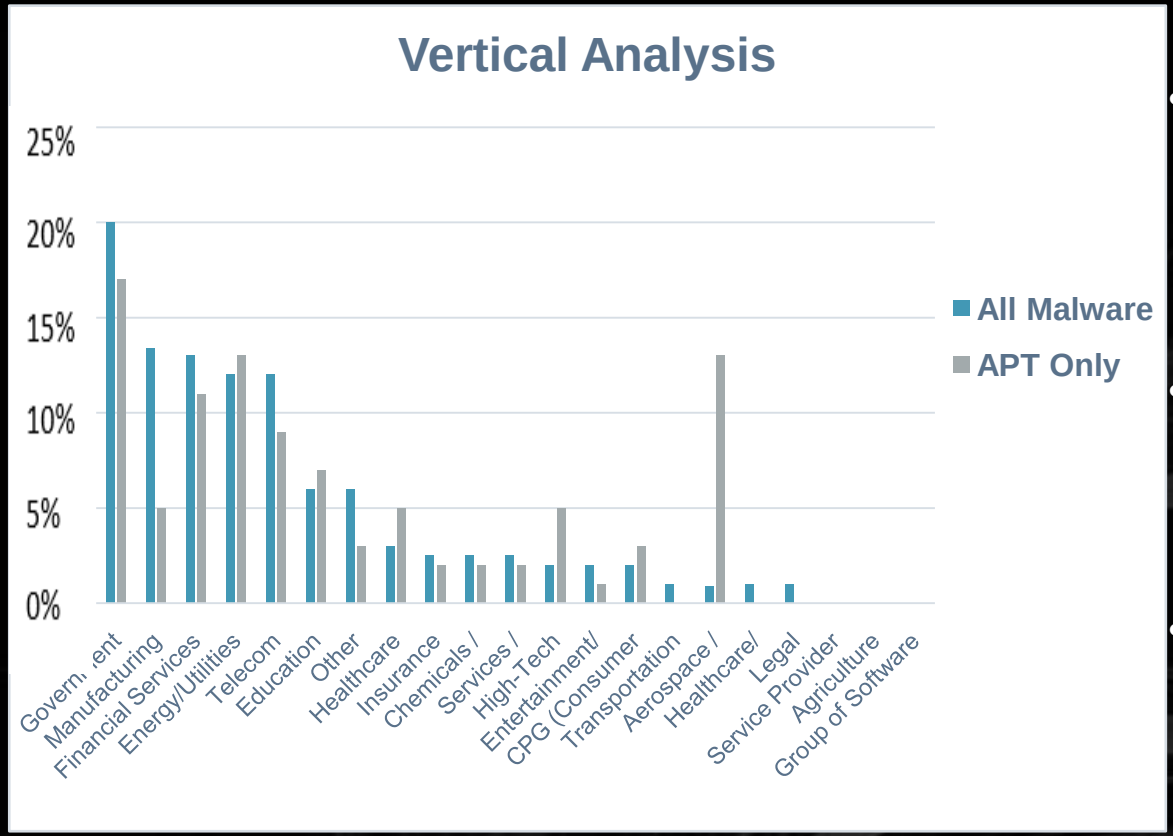
APT Malware Families



- Link specific malware use to cyber threat actors or threat types.
- Then you will aid in the attribution and more effective response strategy.
- APT.LV was the most voluminous tools used.

FireEye

Vertical Analysis



- Energy/Utilities, Healthcare, High Tech, Consumer, & Aerospace and Defense have higher volumes of APT.
- Manufacturing vertical most impacted by crimeware malware as oppose to APT.
- Government, Aerospace & Defense, Financial Services and Telecom verticals represent >50% of total APT detection.

FireEye

Vertical Deep Analysis - Government

- Continue facing threats from financially motivated cyber threat actors looking for personal or sensitive data. (citizens data, revenue data, and other)
- Cyber espionage risks from state-sponsored cyber threat actors.
- Middle East with its political volatility and large oil and mineral reserves will employ cyberespionage capabilities to monitor their economic, political and military interest.
- Cyber threat actors are moving laterally for an initial compromise at a financial institution and gain access to the networks of other departments in the government.
- APT. Kaba is the most prevalent threat within the government sector:
  - Preferred tool for many Chinese inferred APT groups
  - AKA APT.plugX, Backdoor.APT.DestruRat, Trojan.APT.PlugX, Backdoor.APT.SOGU , FE_APT_Choiceguard_Kaba
  - Malware is capable of file upload and download
  - Implement custom protocol to provide C&C server with graphical access to the victim system

Vertical Deep Analysis - Government

- APT. Kaba is the most prevalent threat within the government sector:
  - Backdoor provides threat actors with SQL data base querying capabilities using HTTP POST request or custom binary requests.
  - Backdoor delivered through web compromise and phising emails.
  - This backdoor is currently actively used by Chinese based APT groups : APT9, APT10, APT17, APT20, APT22, APT26 & APT27.
- APT.RunBack
  - Targeting Turkish intelligence entities
  - Attribution has been leveled at a ME Country

Vertical Deep Analysis – Financial Services

- China based APT actors seeking to support economic reforms and reach state goals.
- Financial threat actors seeking financial gain through direct theft of funds. .
- Disruptive threat actors and hacktivists seeking publicity, divert bank's attention and demonstrate political motive.
- APT. LV is the most prevalent threat within the financial services sector:
  - Malware publicly available NjRAT capable of keystroke logging, credential harvesting, reverse shell access, file uploads and downloads and file and registry modifications.
  - Allow threat actors to create new variants based on configurations of C&C servers, specified filenames, options to spread via USB and othe customization options.
  - Middle Eastern and African threat actors are using this malware

FireEye

Vertical Deep Analysis – Aerospace/Defense

- Threat actors affiliated with nation state and motivated by military and economic interests.
- Steel intellectual property and proprietary information.
- Damage or disrupt the function of critical technologies and systems
- Used in a war scenarios that would likely deny the adversary the use of the affected military systems.
- APT. NS01 is the most prevalent threat within the Aerospace/Defense sector:
  - Proxy aware tool
  - Employ several evasion techniques
    - Specifies fake properties pretending to be Google or MSFT
    - It is 41MB is size and the cyber investigator will be discouraged from taking a closer look.

FireEye

Conclusion & Recommendations

- Assume your organization is a target and your security controls are compromised
- Establish a cyber risk framework with board level sponsorship.
- Establish an IR service in a SOC/CIRT team to detect and react to APT events quickly.
- Enhance your visibility with external cyber threat intelligence.
- Bring in the right technology that could identify APT.