FireEye

Threat Landscape

Israel 2013

Document Control

Document information

Version	1.4
Title	Threat Intelligence / Israel 2013
Creation Date	17 January 2014
Revision Date	27 January 2014

Contact information

Name	Title	Email
Alexander Haik	Regional Sales Director Israel	alexander.haik@fireeye.com
Dud Akiva	Systems Engineer	dudu.akiva@fireeye.com
Yogi Chandiramani	Director Systems Engineering Europe	yogi.chandiramani@fireeye.com

Table of Contents

Introduction

We appreciate the opportunity to provide you with a unique insight into the Threat Landscape in Israel for 2013. For many years, we have been stating that over 95% of businesses unknowingly host compromised PC's within their corporate networks. Israel is no different than any other country. During this assessment, we have identified all types of threat actors: nation state, cyber criminals, activists and "amateurs" as well.

Well-funded threat actors have adjusted their techniques from generic, opportunistic and scattershot to targeted, resilient and evasive. It is my pleasure to present this analysis that provides a comprehensive assessment of the Israeli threat landscape.

I am looking forward to discuss this report with you and help you define and execute your cyber security strategy for 2014 and beyond.

Best Regards,

Alexander Haik,
Regional Sales Director, Israel

Executive Summary

This FireEye Advanced Threat Report for Israel provides an overview of the advanced persistent threats (APT) targeting computer networks that were discovered by FireEye during 2013 in Israel.

This report summarizes 2013 data gleaned from the FireEye Dynamic Threat Intelligence (DTI) cloud of worldwide malware protection platforms. Based on this information and insight, FireEye can report the following:

- **More than 52,000 events were discovered in 2013 in Israel across 20 organizations**
- **More than 2,000 end points** were probably compromised as they were beaconing or communicating with CnC servers
- **More than 272 variant of malwares** were detected in 2013
- **The number of APT events represented 25% of all events identified or 1.5 APT event per hour in 2013**
- **40 variant of APT** were identified in 2013
- **The Defense/Airlines industry is the most targeted vertical** representing on its own over 50% of compromised end points with APT
- **The USA is currently home for more than 50% of callbacks coming from Israel**
- We identified almost **1,000 malicious files** focusing on obfuscation techniques to bypass signature based controls

Disclaimer: This report only covers computer network attacks that targeted FireEye customers, sharing their metrics with FireEye – it is by no means an authoritative source for all APT attacks in Israel and elsewhere in the world. In this dataset, we take reasonable precautions to filter out "test" network traffic as well as traffic indicative of manual intelligence sharing among our customer base within various closed security communities. We realize that some popular APT TTPs can be reused and repurposed by both cyber-criminals and nation-state threat actors alike. To address this issue, we employ conservative filters and crosschecks to reduce the likelihood of misidentification.

Definitions

Advanced Persistent Threat (APT): a distinct set of cyber tools, techniques, and procedures (TTPs) that are employed directly or indirectly by a nation-state or a sophisticated, professional criminal organization for cyber espionage or the long-term subversion of adversary networks. Key qualifying APT characteristics include regular human interaction (i.e. not a scripted, automated attack), and the ability to extract sensitive information, over time, at will.

Callback: an unauthorized communication between a compromised victim computer and its attacker's command-and-control (CnC) infrastructure.

Remote Access Tool (RAT): software that allows a computer user (for the purposes of this report, an attacker) to control a remote system as though he or she had physical access to that system. RATs offer numerous attractive features such as screen capture, file exfiltration, etc. Typically, an attacker installs the RAT on a target system via some other means such as spear phishing or exploiting a zero-day vulnerability, and the RAT then attempts to keep its existence hidden from the legitimate owner of the system.

Security Event: FireEye regularly discovers a wide variety of web, email, and file-based threats, including the opening of a malware attachment, a click on a malicious hyperlink, or the "callback" of an infected machine to its attacker's command-and-control (CnC) network.

Targeted attack: a unique TTP-to-Target pairing. Please note, that APTs usually employ multiple TTPs and manage multiple targeted attacks at the same time.

Threat Actor: the nation-state or criminal organization behind an APT. This could be a military unit, an intelligence agency, a contractor organization, or a non-state actor with indirect state sponsorship.

Tools, Techniques, and Procedures (TTPs): the characteristics specific to a threat actor in the cyber domain, usually referring to specific malware. As a caveat, it is important to remember that APTs normally employ multiple TTPs, and multiple APTs can also use the same TTPs. This dynamic frequently complicates cyber defense analysis.

Vertical: one of FireEye's 20 distinct industry categories: Aerospace, Chemicals, Construction, E-Commerce, Education, Energy, Entertainment, Finance, Government, Healthcare, High-Tech, Insurance, Legal, Manufacturing, Other, Retail, Services, Telecom, Transportation, and Wholesalers.

Target: the recipient of an APT attack. In most cases, the low "false positive" rates inherent in FireEye alerts suggest that the discovered attack was successful.

Malware Distribution

Introduction

The number of events has grown by a 4x factor between January and December 2013. The number of APT has more than doubled over the year. We identify sporadic spikes and downturns:

- **April/May 2013**: Possibly due to an Anonymous campaign *(#op-Israel)* launched against Israel during April. Alternatively, A Syrian organization launched an attack at Israeli infrastructure as a retaliation for reported Israeli bombing in Syria.
- **September 2013**: Jewish New Year holidays which lasted through September and whereby threat actors can take full advantage of festivities to better infiltrate organizations.

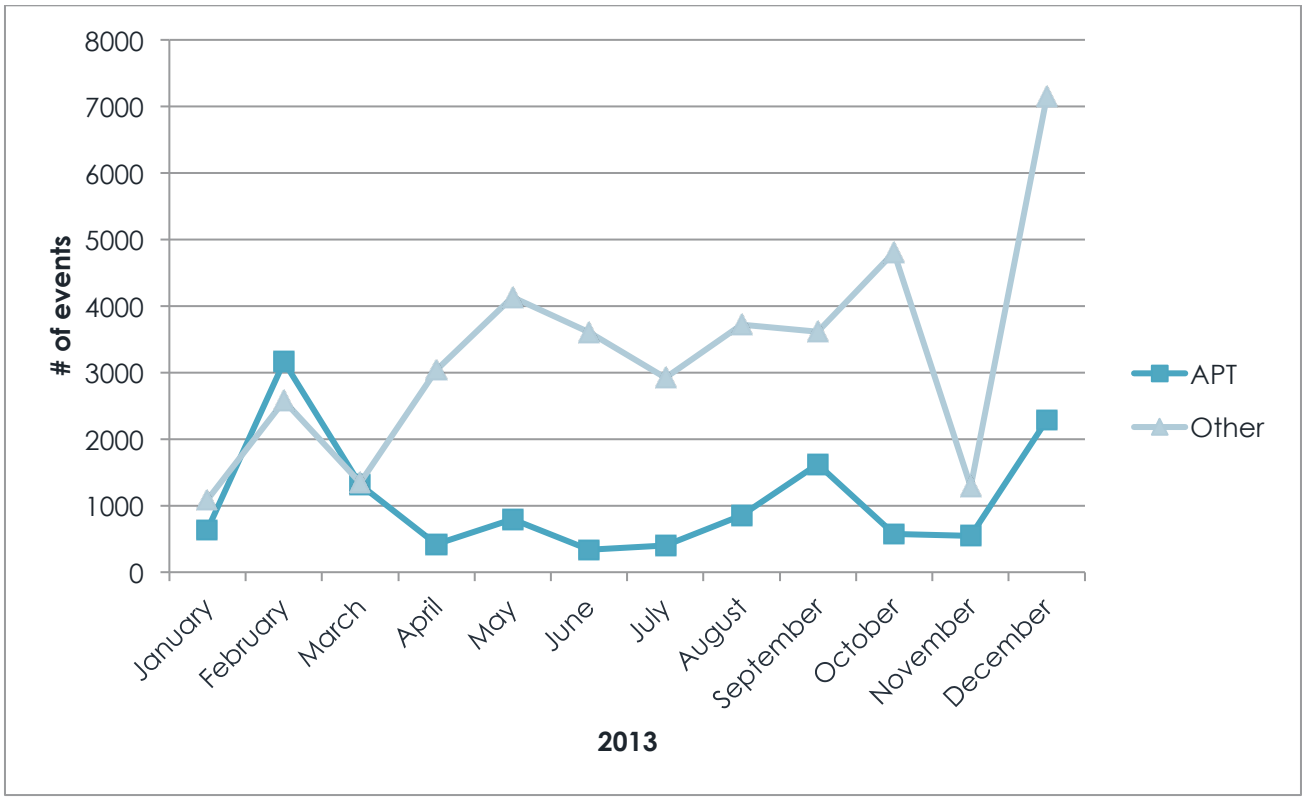


Figure 1 – Malware Trending

For the month of December 2013, we identified more than 3 APT events/hour.

Detection Type Distribution

The following figure presents the Detection Type distribution based on the malware family.

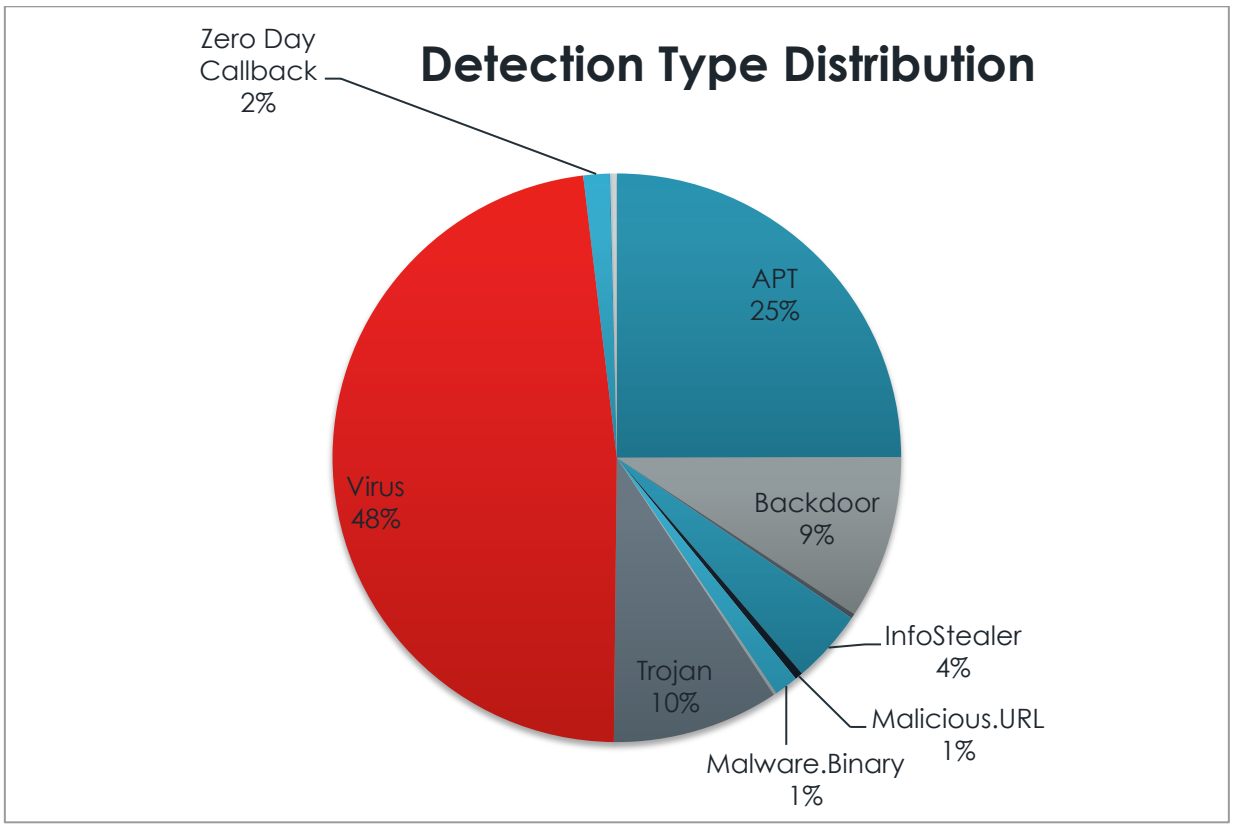


Figure 2 – Detection Type Distribution

The Virus family leads the chart with 48% of overall number of events identified in 2013. This number is particularly interesting as this family of malware is typically recognized by signature-based technologies. While a virus does not typically steal information, it is designed to replicate itself within the organization causing disruption and nuisance.

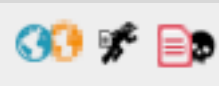
On the other hand of the spectrum, APT and Remote Access Toolkit represents more than 25% of the distribution. These malware families take complete control of workstations located in organizations and not only steal data but also are very sophisticated by nature. They typically move laterally within the organization by using the compromised workstation as a stepping-stone.

Trojan, Backdoor and Infostealer represent almost 23% of the overall distribution. These families of malware have an objective which is to take control of your workstation and typically steal sensitive data. The level of sophistication and commitment is however less than APT.

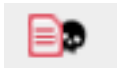
Zero day malware represent 4% of the overall distribution. Those are typically not identified with signature-based tools and therefore bypass the legacy security controls.

APT families

The following table presents the most popular APT families identified during this assessment::

Family	Description	Attributes
Gh0stRat	Gh0stRAT is a malicious remote administration tool (RAT). Requiring little technical savvy to use, RATs offer unfettered access to compromised machines. They are deceptively simple—attackers can point and click their way through the target's network to steal data and intellectual property. But they are often delivered as key component of coordinated attacks that use previously unknown (zero-day) software flaws and clever social engineering. Features common to most Windows-based RATs include key logging, screen capturing, video capturing, file transfers, system administration, password theft, and traffic relaying.	
Beebus	FireEye discovered the Trojan.APT.Beebus APT campaign consistently targeting companies in the aerospace and defense industries. The campaign has been in effect for sometime now. This campaign uses both email and drive-by downloads as a means of infecting end users. The threat actor has consistently used attachment names of documents/white papers released by well-known companies. The malicious email attachment exploits some common vulnerabilities in PDF and DOC files. The malware uses a well-documented vulnerability in the Windows OS known as DLL search order hijacking. There is an order in which executables load DLLs on the Windows operating system. This particular malware takes advantage of this vulnerability and drops a DLL called ntshrui.DLL in the C:\Windows directory. The first place from where the executable looks to load the DLL is its own directory. By dropping the ntshrui.DLL in the directory C:\Windows, the malware achieves persistence More information can be found at: http://www.fireeye.com/blog/technical/targeted-attack/2013/02/operation-beebus.html	
LV	Backdoor.APT.LV primarily uses websites hosting .EXEs to propagate. Many of the domains used names referring to the Middle East. The malware was observed talking back to its CnC using a custom protocol over port 80. The malware gathers the information from the compromised machine and sends it to its CnC: Netbios name, User, Date, Locale, Windows OS name. The malware also informs the CnC of its version. Although the	

	Backdoor.APT.LV collects crucial information pertaining to the user and the compromised machine, upon execution, it also (oddly) opens up a dialog box asking the user to run an executable named "Trojan.exe." This obvious name of a malicious executable suggests this malware is intended for non-native English speakers More information can be found at: http://www.fireeye.com/blog/technical/botnet-activities-research/2012/09/the-story-behind-backdoorlv.html	
ExtremeRAT	XtremeRAT is a malicious remote administration tool (RAT). Requiring little technical savvy to use, RATs offer unfettered access to compromised machines. They are deceptively simple—attackers can point and click their way through the target's network to steal data and intellectual property. But they are often delivered as key component of coordinated attacks that use previously unknown (zero-day) software flaws and clever social engineering. Features common to most Windows-based RATs include key logging, screen capturing, video capturing, file transfers, system administration, password theft, and traffic relaying.	
PoisonIvy	Well known APT – introduced by the PLA http://www.fireeye.com/blog/technical/cyber-exploits/2013/09/hand-me-downs-exploit-and-infrastructure-reuse-among-apt-campaigns.html	

 Decoy Document

 Browser Tempering

 Performs Data theft

 Exhibits Backdoor Capabilities

These APT families are highly sophisticated and motivated. Their business impact is typically very high.

Callback Analysis for Israel

The following map highlights the locations of the CnC Servers identified in this threat analysis. All these callbacks originated from Israel.

More than 50% of all callbacks from Israeli victims appear to contact 1st tier CnC nodes based in the USA and 7% of callbacks appear to contact 1st tier CnC nodes based in China.

It is interesting to note that most callback destinations are within western countries, where Israel is regarded more positively.

Figure 3 – Callback Map

Vertical Analysis

Let's first have a look at industry verticals, each of which possesses substantial intellectual property value. Furthermore, these verticals often play a tangible role in cybercrime and national security affairs. The following verticals were analyzed in the assessment.

Defense/Airlines: this vertical designs and operates military equipment or operates commercial or defense air transport.

Automotive/Transportation: this vertical designs, builds, and operates cars, which have myriad commercial applications.

Chemicals: chemistry is the study of matter, and plays a central role in bridging all of the natural sciences, including their relationship to energy.

E-Commerce: online web services to sell products to businesses or consumers.

Energy: in physics, energy is required for any kind of "work," to include starting engines, turning on city lights, or launching a missile.

Entertainment/Media/Hospitality: organizations providing information and recreation services.

Finance: most financial transactions today are conducted via the Internet, whether between people, businesses, or governments.

Manufacturing: Providing facilities to build products for other verticals.

Other: some specialized businesses play a niche role in national economies, but are nonetheless targeted by niche-focused APTs.

Pharmaceuticals: medicine industry, providing products for healthcare.

The following figure presents malware activity by verticals.

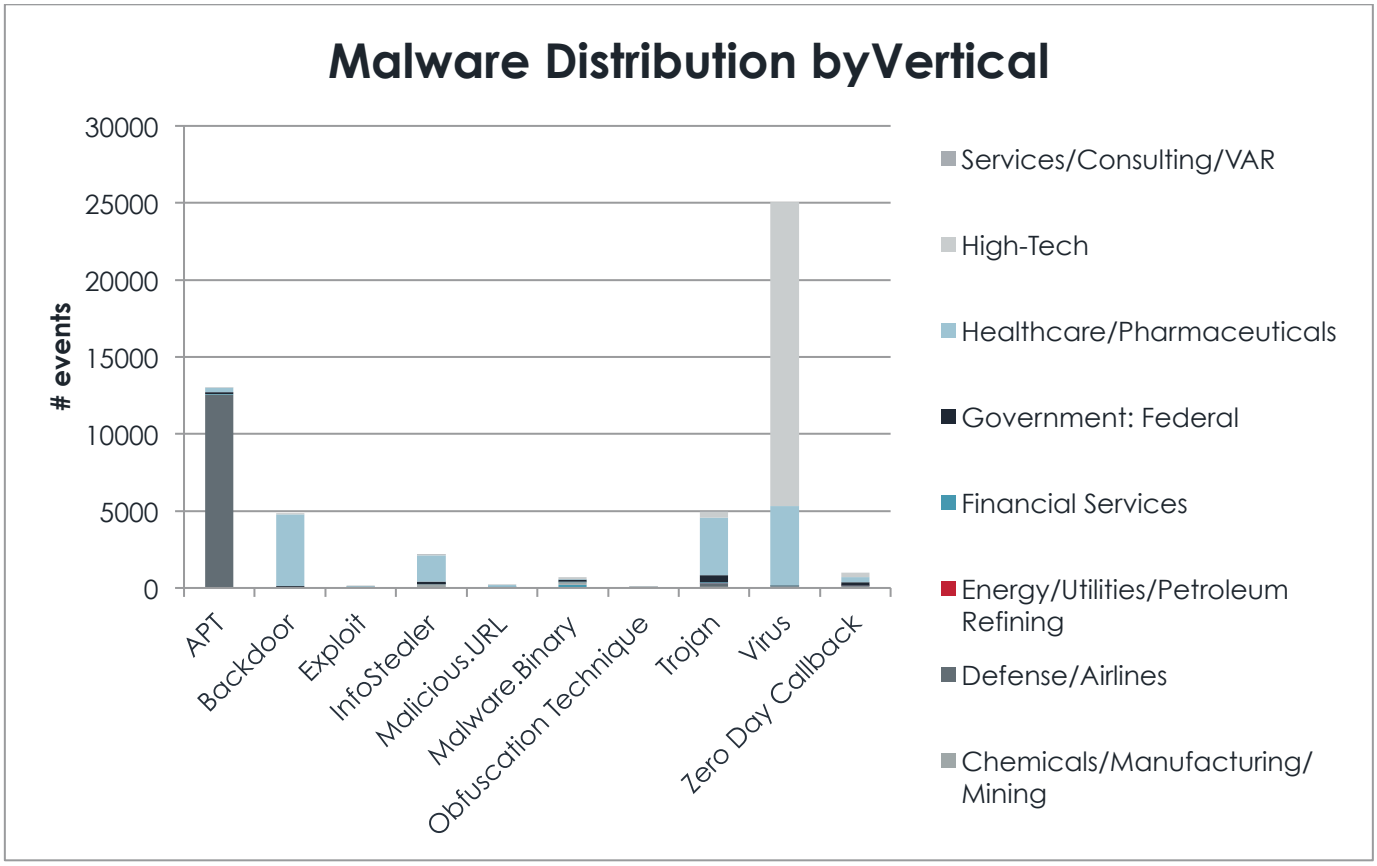


Figure 4 – Malware Distribution per Vertical

It is clear that high value verticals are being targeting with High Tech leading the group, closely followed by Health Care/Pharmaceuticals vertical.

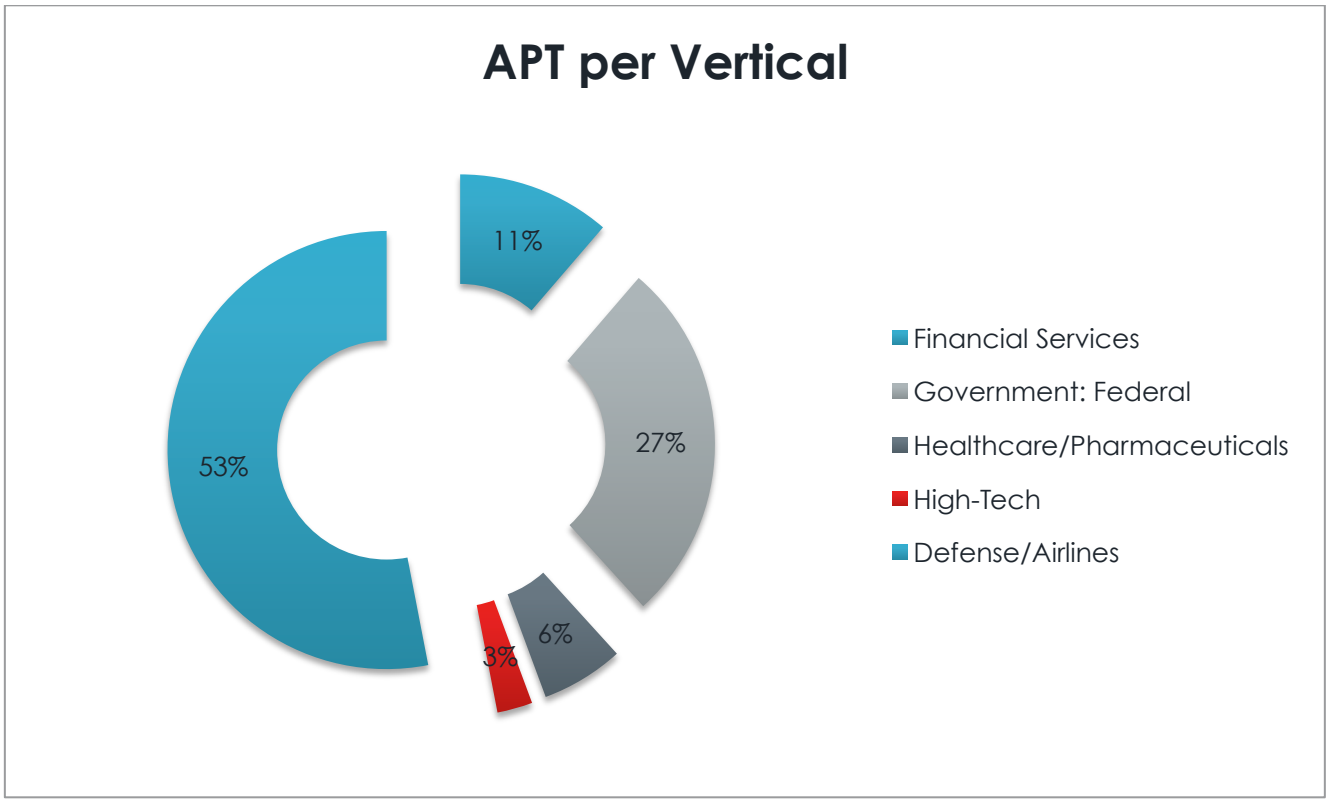


Figure 5 – APT distribution per vertical

Looking more specifically at APT events, the Defense/Airlines vertical represents on its own more than 50% of compromised end points. The following table presents the APT families identified for the Defense/Airlines vertical:

APT Name for Defense/Airlines vertical
Check_Command
DarkComet
MdAdum
Mirage
Mongall
Page
Zegost
9002
Beebus
Cresy
PingBed
Taidoor

Figure 6 – APT name for Defense/Airlines Vertical

Government vertical is not spared with about 27% of compromised end points.

The following table presents the APT families identified for the Government vertical:

APT Name for Government vertical
1PHP
DarkComet
FakeMessenger
Gh0stRat
Kaba
Lurid
LV
Note
Protux
XtremeRAT
Bosee
Generic
Suroot
WMIGhost

Figure 7 – APT Name for Government vertical

Conclusion and Recommendations

The evidence highlighted in this report demonstrates that organizations in Israel are a target for advanced threats. The type of malwares identified is consistent with what we see in other countries and verticals. Attackers are targeting high value organizations in Israel and are making their way in. The high number of APT events suggests a large level of information theft.

Our recommendations are the following:

1. Ensure existing security tools are up to date – the evidence of Virus family malware can be easily addressed with legacy, signature based tools
2. Implement Advanced Threat Protection systems to ensure high value data is safe guarded
3. Plan and Implement an Incident Response and Management strategy to close existing security gaps
4. Share and collaborate with other entities in terms of emerging cyber threats to optimize your security posture