



REGIONAL ADVANCED THREAT REPORT

Europe, Middle East and Africa
1H2014

SECURITY
REIMAGINED

TABLE OF CONTENTS

Executive Summary 3

Definitions 4

Trend 5

APT Detection 6

 Country Analysis 6

 Vertical Analysis 9

 APT Malware Families 11

Conclusion and Recommendations 19

Executive Summary

This FireEye Advanced Threat Report for EMEA provides an overview of the advanced persistent threats (APT) targeting computer networks that were discovered by FireEye during the first half of 2014 in EMEA.

Motivated by numerous objectives, threat actors are evolving the level of sophistication to steal personal data and business strategies, gain a competitive advantage or degrade operational reliability.

This report summarises first half of 2014 data gleaned from the FireEye Dynamic Threat Intelligence (DTI) cloud. Based on this information and insight, FireEye can report the following:

- **Malware attacks—especially advanced targeted attacks—have nearly doubled in the first half of 2014**
- **The UK and Germany were the most targeted countries**

- **Government, financial services, telecommunications and energy were the most targeted verticals.**

Disclaimer: This report only covers computer network attacks that targeted FireEye (anonymised) customers, sharing their metrics with FireEye – it is by no means an authoritative source for all APT attacks in EMEA 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 realise that some popular targeted threat actors’ tools, techniques and procedures (TTP’s) 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 organisation 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 unauthorised communication between a compromised victim computer and its attacker's command-and-control (C2) 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.

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 organisation believed to be behind an APT. This could be a military unit, an intelligence agency, a contractor organisation, 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 defence analysis.

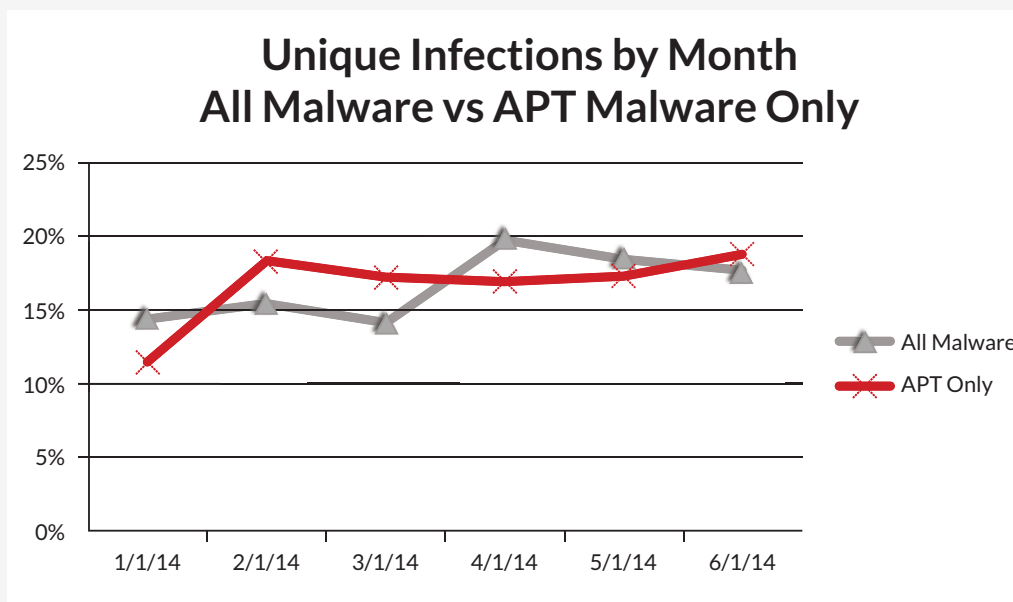
Vertical: one of 20 distinct industry categories: Aerospace, Chemicals, Construction, E-Commerce, Education, Energy, Entertainment, Finance, Government, Healthcare, High-Tech, Insurance, Legal, Manufacturing, Other, Retail, Services, Telecom, Transportation, and Wholesalers.

Trend

Finding: Malware attacks—especially advanced targeted attacks—have nearly doubled in the first half of 2014.

The number of unique infections has been growing steadily in EMEA. However if we focus on targeted attacks (that is, activity we've associated with targeted threat groups or malware known to be used by those groups), the number of unique infections almost doubled between January and June 2014.

Figure 1:
Unique Infections
Trend



APT Detection
Country Analysis

The UK and Germany are the most targeted countries.

Let's first have a look at which countries that have been impacted by APT malware in EMEA.

The highest number of APT malware detected in EMEA in first half of 2014, by country, can be summarised:

- 1. United Kingdom (17%)
- 2. Germany (12%)
- 3. Saudi Arabia (10%)
- 4. Turkey (9%)
- 5. Switzerland (8%)
- 6. Italy (6%)
- 7. Qatar (5%)
- 8. France (4%)
- 9. Sweden (4%)
- 10. Spain (3%)

Figure 2:
APT Detection by
Country

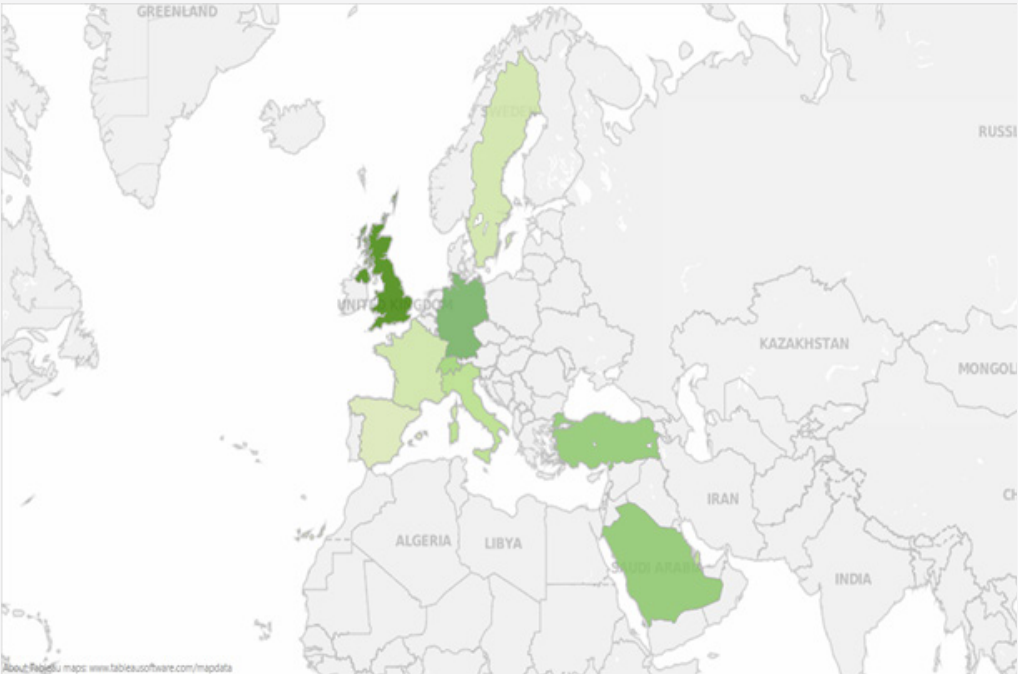
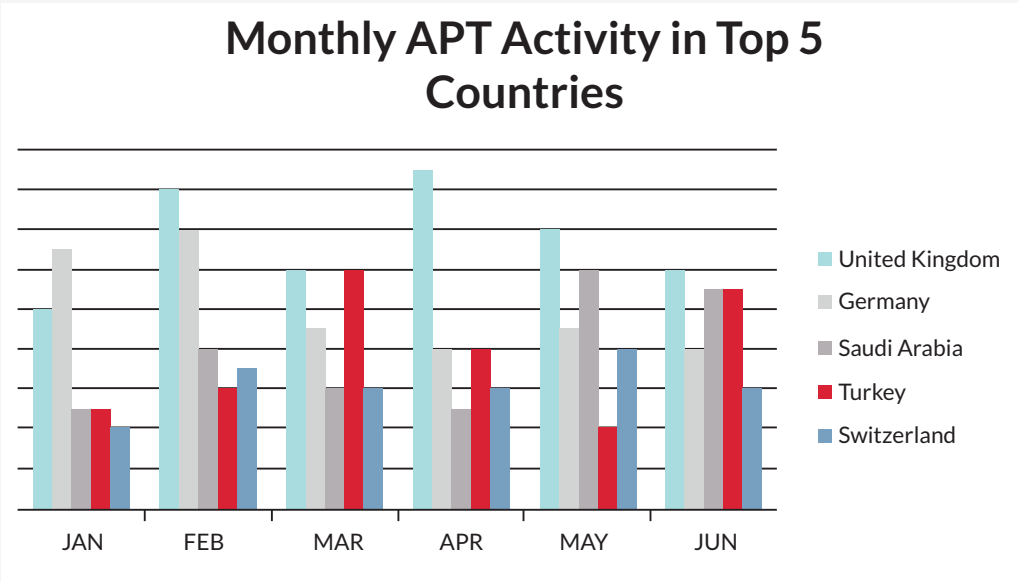
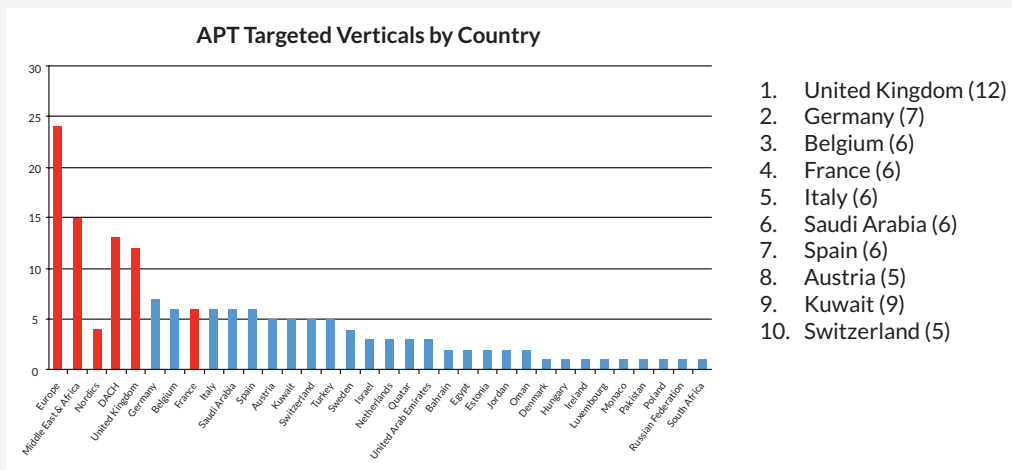


Figure 3:
Monthly APT Activity
in Top 5 EMEA
countries



Comparing on an EMEA basis, we have identified that UK, Germany, Italy and France have the largest number of verticals targeted by APT.

Figure 4:
Number of Verticals
Hit By APT Malware
by Country



We have also grouped specific EMEA sub regions:

- Europe (all European continent countries)
- Middle East & Africa (all Middle East and Africa countries)
- Nordics including Sweden, Denmark, Finland and the Baltic States
- DACH including Germany, Austria and Switzerland

Interestingly UK and DACH have similarities in the number of verticals targeted and also in terms of monthly activity highlighted in Figure 4. This suggests that a specific country is not being targeted but rather specific verticals.

Vertical Analysis

Government, financial services, telecommunications and energy were the most targeted verticals.

The following figure presents APT activity, measured by number of alerts, by vertical.

Government, Financial Services and Telecom verticals represent more than 50% of total APT detections, and all are considered strategic industries.

The following paragraph provides an in depth analysis of the top four verticals impacted.

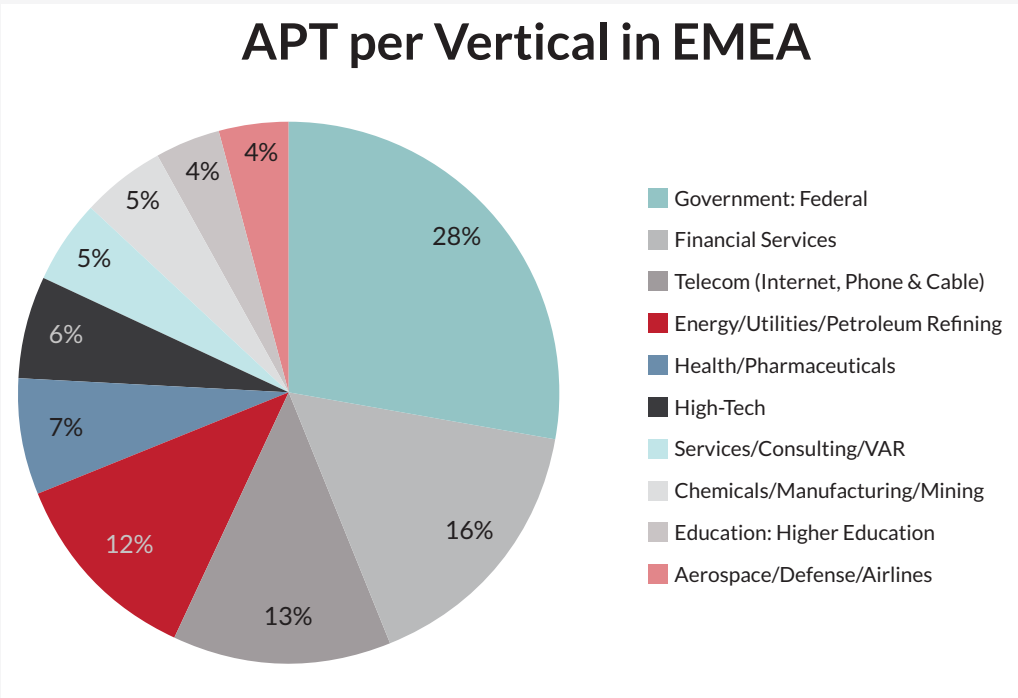
Government:

Based on these findings we expect that government agencies and institutions will likely continue to face threats from financially

motivated threat actors who are in search of personal or sensitive data. Central agencies and institutions that maintain citizens' data, like departments of revenue, are likely to be particularly at risk, due to the potentially valuable information stored on their networks. Local government entities may additionally face threats from cyber actors interested in testing their own skills or foreign government network defences.

Organisations in EMEA are almost certain to face cyber espionage risks from state-sponsored or state-associated threat actors working for or in association with nation-state governments. The Middle East in particular is one of the most politically volatile regions in the world and boasts some of the world's largest oil reserves, making it an area of strategic focus for many states outside the region. These countries almost certainly will

Figure 5:
APT Malware
Detections per
Vertical



employ cyber espionage capabilities to monitor their economic, political, and military interests, which will likely drive the further development of local cyber espionage efforts.

Agencies and institutions whose networks are connected to those of other local government entities also face potential risks from threat actors moving laterally from an initially compromised network. In a case study, we noted that the threat actors were able to move laterally from an initial compromise at a financial institution and gain access to the networks of other departments in the state. However, this group was also able to compromise the network of a local government outside of the original geography.

We suspect that a nation state actor may opt to target a local government network as opposed to that of a central government entity as the local network poses an easier and less complex target. Local governments likely lack the resources for stringent network security and monitoring, making them a technically easier target for threat actors. However, despite the relatively lax network security, local government networks also likely contain potentially valuable information for nation state threat actors, including insight into major industries operating within their jurisdictions, as well as personnel and financial data.

Financial Services:

FireEye suspects the large amount of activity in the sector is partly due to the diverse motivations of threat actors in the industry, to include (1) China-based APT actors seeking to support economic reforms and reach state goals, (2) financial threat actors seeking to financial gain through the direct theft of funds of the indirect

theft of information to be sold, and (3) disruptive threat actors and hacktivists seeking to gain publicity, divert banks' attentions, or demonstrate a political motive. Any one of these threats would increase activity in an industry, but the presence of all three likely accounts for the large number of intrusions in the financial services industry.

Additionally, as financial advisors are often at the heart of the mergers and acquisition process, this is a sensitive time for organisations seeking to maintain some level of secrecy. It is also a potential strategic intelligence opportunity for threat actors seeking to collect valuable information and insights. FireEye has observed a number of APT groups target organisations during the mergers and acquisitions process.

We suspect that the threat actors conducted these operations in order to collect information that would prove advantageous during subsequent contract negotiations with the targeted organisations, as well as information collection for possible foreign government scrutiny and insight.

Candidate organisations with unidentified intrusions and unaudited networks pose a risk for any acquiring organisation. These risks include subsequent financial and reputational damage to parent organisations, and extending the possibility of spreading an existing compromise to the acquiring organisation's networks. Though for a different purpose, FireEye has observed APT groups target and compromise a target organisation's circle of providers, partners, and advisors as a means to leverage any bridged networks and gain access to the target organisation.

Energy:

We have observed threat actors using HAVEX/PEACEPIPE malware to try and compromise energy targets; Nordic energy companies and an EMEA state's national oil company have been recent targeted. We believe that multiple actors operating out of Russia are behind these campaigns.

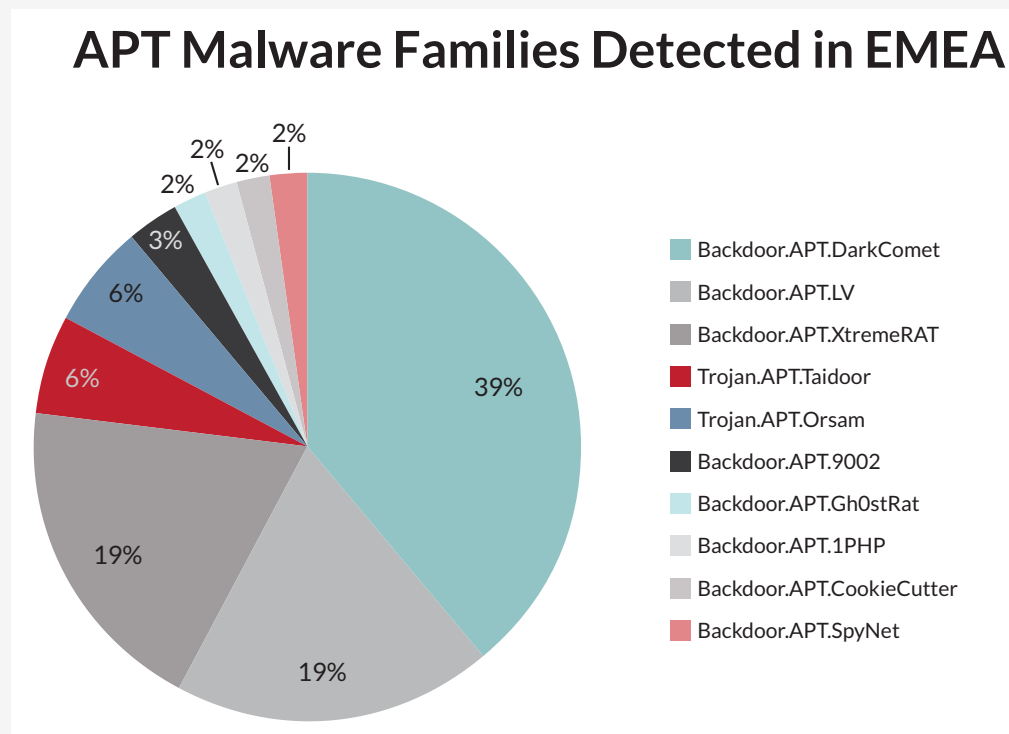
APT Malware Families

The following graph represents the distribution of targeted malware families identified in the first half of 2014. The malware families are important to track from a risk perspective, as each family has different capabilities and risks to consider. This becomes significant when we can link specific

malware use to threat actors or threat types, which aids in attribution and enables people to respond more effectively.

DarkComet, njRAT (LV), Taidoor, and XtremeRAT were the malware variants that FireEye appliances in the EMEA region detected the most frequently. DarkComet, njRAT, and XtremeRAT are all publicly available, easy-to-use RATs—njRAT is particularly popular in the region, and its author is based in Algeria. As such, they could be used by advanced attackers to “blend in”, but they could also be employed by different types of threat actors with all manner of motives because of their ease of access and low barrier to entry. In addition, we have only observed suspected and confirmed

Figure 6:
APT families
detected in EMEA



China-based APT groups use Taidoor. The clients affected by this alert, all of which were in the federal government or energy industry verticals, track closely with the targeting pattern of the confirmed APT group, giving further credence to our belief that Chinese threat actors conduct cyberespionage against organisations in this region.

Rather than building custom malware and exposing valuable zero day exploits, many threat actors behind targeted attacks use publicly or commercially available remote access Trojans (RATs). This pre-built malware often has all the functionality needed to conduct cyber espionage and is controlled directly by the threat actor, who frequently possess the ability to adapt to network defences. As a result, the threat posed by these RATs should not be underestimated. On any given day detection by traditional security solutions for these well-known RATs varies widely – some may be well-known and detected quickly, others will remain undetected for months.

However, it is difficult to distinguish and correlate the activity of targeted threat actors based solely on their preference to use particular malware – especially freely available malware. From an analyst's perspective, it is unclear whether these actors choose to use this type of malware simply out of convenience or in a deliberate effort to blend in with traditional cybercrime groups, who also use these same tools.

DarkComet, for example, has been available for

free since 2008. It is popular on a variety of underground forums and used by a wide range of actors for many purposes. (After reports indicated that DarkComet was used in connection with the conflict in Syria, the creator of DarkComet, DarkCoderSC, created a removal tool and ultimately quit developing the RAT).

Although publicly available RATs are used by a variety of operators with different intents, the activity of particular threat actors can still be tracked by clustering command and control server information as well as the information that is set by the operators in the builder. These technical indicators, combined with context of an incident (such as the timing, specificity and human activity) allow analysts to assess the targeted or non-targeted nature of the threat.

FireEye studied a sample 100 active CnC domains for njRAT (includes LV categorisation), XtremeRAT, njw0rm, h-worm, and DarkComet that threat actors used against our customers. Though advanced threat actors are also using these tools, we surmise that various individual hackers and hacking teams are largely conducting these activities for notoriety hacking, hacktivism, cybercrime, or hobby hacking, and not targeted data theft from an APT campaign. Domain resolutions for the 100 dynamic CnC fully qualified domain names (FQDNs) revealed more than 20,000 historical IP resolutions, suggesting that these actors use dynamic domains for connectivity via their local Internet service provider to their personal computers.

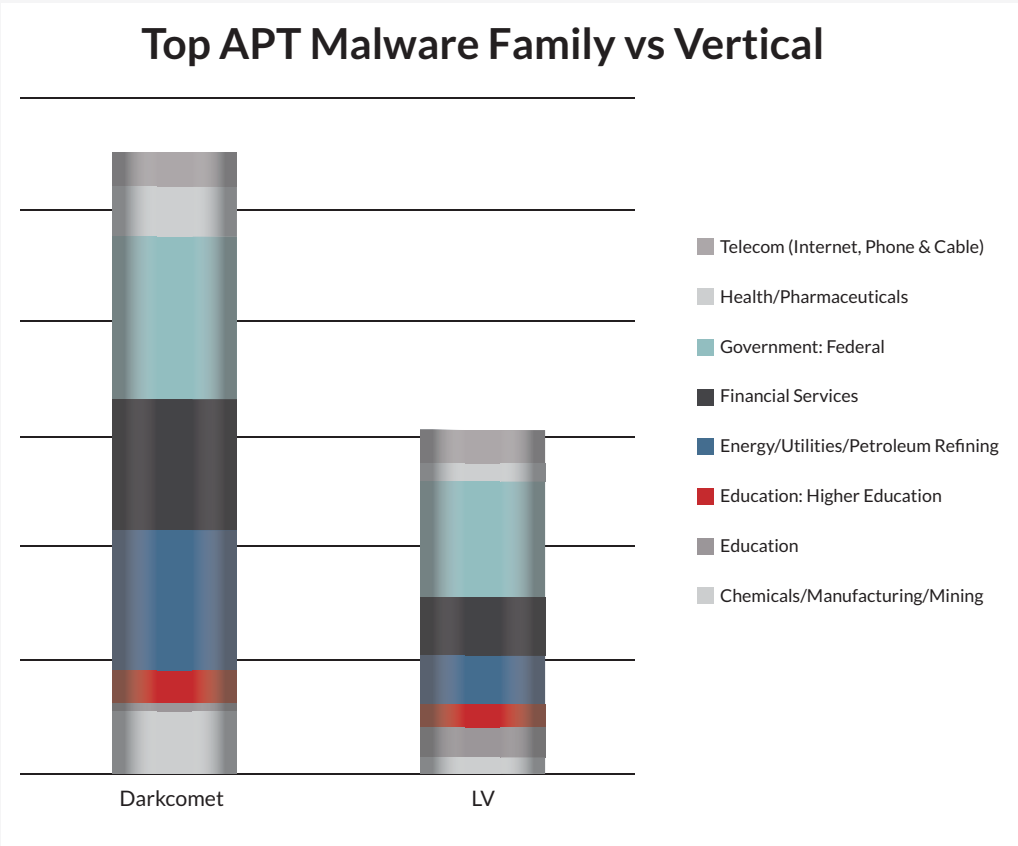
Nearly all the C2s domains used a dynamic domain name system, such as no-ip, dyndns, adultdns, zapto, sytes, servequake, myvnc, with a number of the FQDNs individually resolving to hundreds of IP addresses. The sample set of FQDNs resolved to more than 20,000 IP addresses in our historical data and possibly indicated the origins of the activity given the apparent direct use of local Internet service providers. For example, in one case involving more than 600 FQDN-IP resolutions, more than 500 of the IPs appeared to be Jordan-based IPs. Figure 1 below shows the primary and secondary countries¹ for FQDN-IP resolutions. FireEye also found cases in which additional FQDNs simultaneously resolved to the same IPs as some of the identified C2 FQDNs.

The extent to which the use of DarkComet, LV and ExtremeRat in attacks that are “targeted”, and not opportunistic, is unclear. They could be targeting an entire industry, simply capitalising on opportunities that arise.

Out of the other malware families detected in EMEA, several of them are confirmed to be in regular use by many different China-based APT groups. These include:

- Taidoor
- Orsam aka DOM
- EXCHAIN
- 9002 aka HOMEUNIX
- COOKIECUTTER aka UPS













Figure 7:
Top APT malware
family vs Vertical





Darkcomet and LV represent more than 50% of identified APT malware families detected in EMEA. Threat Actors are typically organising their attacks through campaigns that target very

specific verticals. If we focus on these two APT families, we find that the Energy and Financial Services have been specifically targeted using the Darkcomet APT.

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. |     |
| 9002 | Trojan.APT.9002 (aka HOMEUNIX) is a backdoor that was linked to an adversary that FireEye has named the Sunshop Group. In the past, FireEye has observed attackers leveraging vulnerabilities CVE-2013-0633 and CVE-2013-0634 to deliver this backdoor. More information can be found at: www.fireeye.com/blog/technical/cyber-exploits/2013/02/lady-boyle-comes-to-town-with-a-new-exploit.html |     |
| ExtremeRAT | XtremeRAT is an openly available remote access tool (RAT). The author(s) is unknown, but they advertise the RAT for €350 via PayPal/Western Union. The tool is offered in three different languages; Portuguese, Spanish, and English, with several unique built-in features such as Windows 8 compatibility, opening/closing CD/DVD peripherals, hiding icons, pausing mouse movements, IRC chat functionality, in addition to other more commonly seen RAT capabilities such as key logging and file uploads/downloads. The developer also appears to be actively improving the RAT and offers free updates to paying customers through their website. The payload itself is UPX packed and coded mostly in Delphi, with communications to command and control (CnC) servers by default over port 81. XtremeRAT has previously been seen targeting international government institutions in the U.S., U.K., Turkey, Slovenia, Macedonia, New Zealand, Latvia, Palestine and Israel; most notably, Israeli Police computers were infected in October 2012, forcing the entire network offline for a brief period of time. The RAT is also popular among attackers based in the Middle East, commonly seen in attacks by Operation Molerats actors and also believed to be in use by the Syrian government. http://www.fireeye.com/blog/technical/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html |     |

| | | |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Leouncia | <p>Backdoor.APT.Leouncia is a powerful backdoor malware program. Leouncia's CnC payload decryption consists of two major phases. The first part is the formulation of a dynamic permutation table using a variable 128 bit key. This permutation table is further used to decrypt the actual payload. Leouncia hibernates itself for an extended period of time. This hibernation is controlled by a file named "readx". Once this command is received, Leouncia tries to read the "readx" file from the current directory. The file "readx" contains the activation date and time in 'FileTime' format like \HIGH DATE\LOW DATE. Leouncia constructs the system time from it and checks if the current date and time is ahead of or equal to this construct. If not it will hibernate itself until that time comes. Eventually, Leouncia enumerate the running process list, encrypts it, and sends it back to its CnC server. It receives dynamic data from the CnC and writes it to a file specified by the attacker. It reads the attacker's specified file onto the target system and sends its contents back to the CnC. Then the attacker's specified process is applied to the infected system. The given pid (process id) terminates a running process and sends a list of all logical drives back to the attackers. A Windows command prompt is spawned and the attacker runs commands of choice. The attacker specify its commands in response to 'GET' requests and the backdoor component invokes these commands on the Windows command shell and sends the response back to the CnC in the form of a 'POST'.</p> |  |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|

| | | |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| SpyNet | SpyNet 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. |  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|



Decoy Document



Browser tampering



Performs Data Theft



Exhibits Backdoor Capabilities

Cybercrime and Hacktivism:

Non-targeted cybercrime is a growing and serious risk to individuals and organisation in EMEA. As we mentioned before, the authors behind two popular remote access tools (RATs), njRAT and h-w0rm, likely reside in Kuwait and Algeria, respectively. Furthermore, most of the C2 domains associated with these malware are located in the Middle East and North Africa. While we have observed both tools used in targeted attacks against companies in the energy and telecommunications sector, they have also been used in run-of-the-mill phishing and cybercrime attacks as well. Cyber criminals will often harvest credential or financial information through logging keystrokes or grabbing credentials stored by a web browser. Though Microsoft recently seized

more than 20 top-level domains associated with njRAT and h-w0rm botnets, we believe that regional hacktivists and cybercriminals will continue to rely on these tools, due to their ease-of-use and ability to escape detection by anti-virus security software.

In addition, we have observed local forums develop a cybercrime scene similar to what we have observed in China and Russia: forums with malware for sale and technical mentors who offer advice on evading anti-virus software and using dynamic domain hosting. This suggests growing expertise and specialization, which will likely result in more effective intrusions and cybercrime operations.

Hacktivism:

FireEye expects that high-profile organisations in the Middle East and North Africa, particularly government and military entities, face a high risk of targeting by hacktivists based inside and outside the region. Moreover, we expect that military and political conflicts will further escalate this risk.

Though hacktivists have targeted Israel in the past, an increasing amount of attacks targeted Israeli government agencies and media organisations during July, almost certainly due to increased violence between Israel and Hamas. Members of the Anonymous hacker collective, as part of a campaign dubbed #OpSaveGaza, announced they had taken more than one thousand Israeli websites offline over the course of July, including those belonging to the Bank of Israel, the Israeli Ministry of Justice, and Mossad.

The Syrian Electronic Army (SEA), a hacktivist group that formed during the 2011 Syrian protests, probably works with, if not entirely for, the Syrian government. They resolutely support President Assad and an alleged member of the group is the son of a powerful Syrian intelligence

officer. The SEA has proven to be a prolific and public threat group—in one case FireEye's Mandiant Consulting Services team responded to, SEA threat actors targeted a media organisation with spear phishing emails and gained access to the company's Twitter feeds within 24 hours. The SEA has also targeted a variety of media organisations with Trojans such as njRAT and XtremeRAT, and has waded into other conflicts unrelated to the Syrian civil war: The SEA recently claimed responsibility for hacking the IDF's Twitter feed and posting false statements about missiles causing a leak at an Israeli nuclear facility.

Hacktivists have also targeted oil and gas companies in the region, to limited success: One group called "AnonGhost," who claim to be made up of Muslim hackers from around the world, threatened to attack oil companies in Kuwait, Saudi Arabia, and other countries it perceives to be acting in the interests of the United States and Israel. Their operation, however, resulted in little damage, taking only a few websites offline with DDOS. Nonetheless, as Internet access grows in MENA countries, we anticipate local hacktivist movements to grow in popularity and effectiveness.

Conclusion and Recommendations

The evidence highlighted in this report demonstrates that organisations in EMEA continue to be targets for advanced threats. The type of malware identified is consistent with what we see in other countries and verticals. Attackers are targeting high value organisations in (EMEA) and are making their way in. The high number of APT events suggests a large level of information theft.

We recommend the following:

1. Assume you and your organisation is a target and that your existing security controls can be bypassed
2. Establish a cyber-risk framework that enables the business with board level sponsorship
3. Establish an incident response/management service in a SOC/CIRT team to be able to detect and react to an APT event quickly
4. Enhance your visibility with external threat intelligence to understand who might attack you and how to avoid the tools, techniques and procedures they use
5. Bring in the right technology that could identify an APT.