FireEye
SECURITY REIMAGINED

SPECIAL REPORT

REGIONAL ADVANCED THREAT REPORT:

Europe, Middle East and Africa 1H2015

CONTENTS

Executive Summary	3
Definitions	4
Crimeware Trend	4
Top crimeware trend Dridex	6
APT Detection	7
Country Analysis	7
APT Malware Families	7
Vertical Analysis	8
Government:	9
Noteable Case in Government: APT.RunBack	10
Financial Services:	10
The most prevalent tool seen in financial sector is LV / NjRat	11
Energy/Utilities	12
Aerospace/Defense Industry	12
APT.NS01	12
Conclusion and Recommendations	13

EXECUTIVE SUMMARY

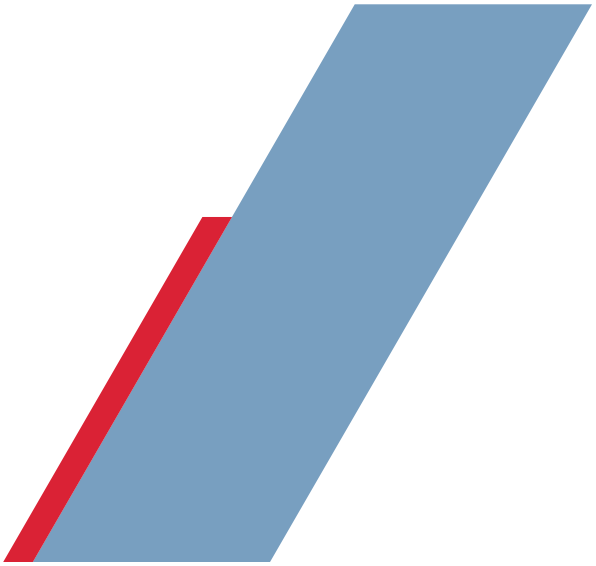
This FireEye Advanced Threat Report for EMEA provides an overview of the advanced persistent threats (APT) targeting computer networks that were discovered by FireEye during the first half of 2015 in EMEA.

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 summarizes first half of 2015 data gleaned from the FireEye Dynamic Threat Intelligence (DTI) cloud. Based on this information and insight, FireEye can report the following:

- Blurring of the lines - Different threat actors sharing tools, techniques and procedures.
- Israel, Saudi Arabia, Spain, UK and Germany are the most targeted countries.
- Energy, Government, Aerospace were the most targeted verticals.

Disclaimer: This report only covers computer network attacks that targeted FireEye (anonymized) 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 realize that some popular targeted threat actors' TTPs (tools, techniques and procedures) 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 (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 organization believed to be 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.

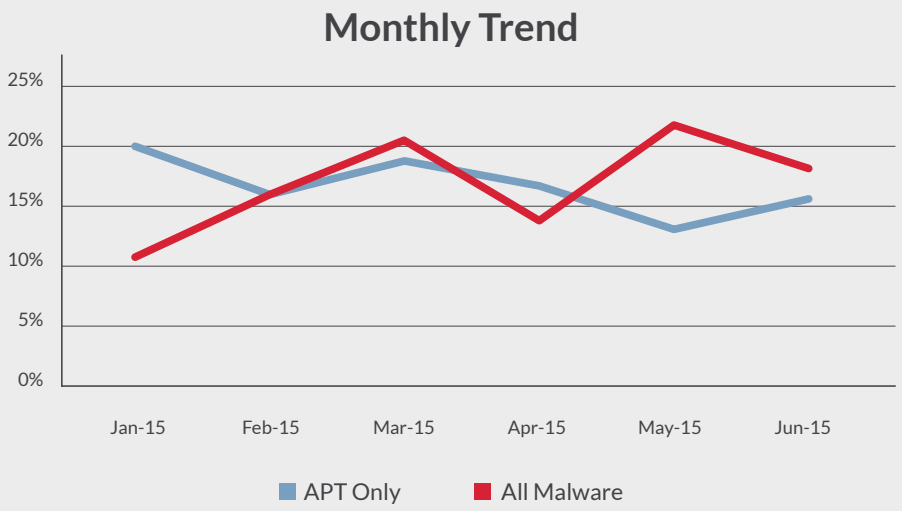
Vertical: one of 20 distinct industry categories: Aerospace, Chemicals, Construction, E-Commerce, Education, Energy, Entertainment, Finance, Government, Healthcare, High-Tech, Insurance, Legal, Manufacturing, Other, Retail, Services, Telecom, Transportation, and Wholesalers.

CRIMEWARETREND

Finding: Malware attacks have nearly doubled in the first half of 2015.

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

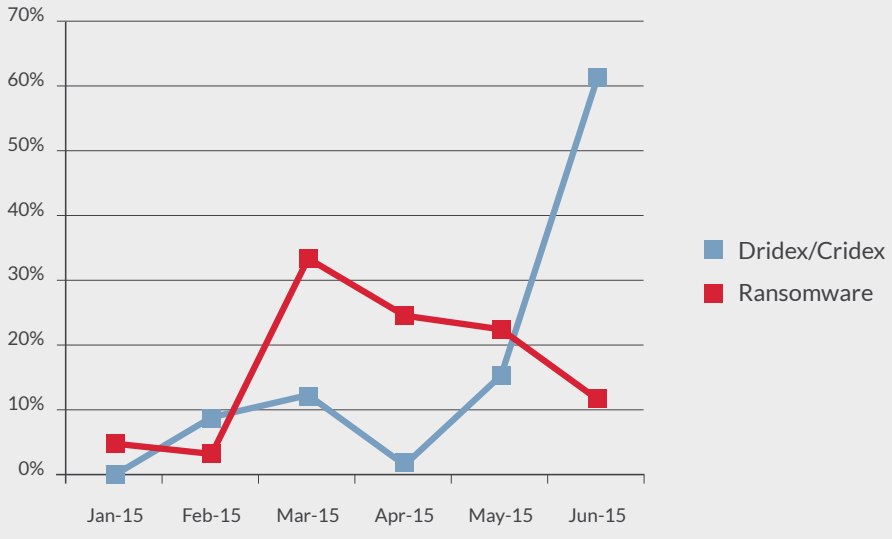
Figure 1:
Unique Infections Trend



The following graphs show the trend for two popular types of crimewarecampaigns:

- Dridex/Cridex
- Ransomware

Interestingly we see the trend for ransomware going down month after month, whereas the Cridex/Dridex campaigns have considerably grown over time. We observed more than 60% of dridex/cridex unique infections just in June 2015. This data suggests that cybercriminals adapt very rapidly to the new techniques as older techniques are detected by security tools.



TOP CRIMEWARE TREND - DRIDEX

We have seen more sophisticated and organized cybercriminal campaigns constantly innovating their evasion techniques for financials purposes. We specifically followed ransomware and dridex malware families evolution during the first half of 2015.

Cridex/Emotet and Dridex are all credential theft trojans. Though primarily used to collect credentials for financial institution websites, threat actors can configure them to capture form submissions to webmail, social networks, or file-sharing sites. An XML-based configuration file specifies which websites the malware should target for collection and which it should ignore.

Threat actors typically distribute these malware variants, using spam emails. Often bearing a subject regarding "invoices," the spam emails contain a malicious XLS or DOC attachment. Within that attachment there can be a macro, a series of commands and instructions, which instructs the compromised system to download a malicious executable, in the case of, Dridex. Once it is installed, Dridex communicates with its command and control (C2) servers. Typically, C2 infrastructure is hosted on a compromised web server running nginx, an open-source HTTP server and reverse proxy, on port 8080, though this can vary by version. Dridex is a new variant of the malware previously known as Cridex/Emotet, Feodo, or Bugat.

Since Dridex requires that macros be enabled in order to infect a system, when the malicious email attachment is opened, if macros are not enabled, it will attempt to social engineer the user into enabling them by displaying a pop-up box suggesting macros be enabled. Users should be cautious when opening any email attachments and seek advice before following instructions that require lowering any security defenses, such as enabling macros.

Credential theft is a booming darkweb business model, credentials stolen will often end upon darkweb markets such as this one.

Clearly focused on selling personal information and financial data. This puts any stolen credential data into the hands of other threat actors.

APT DETECTION

Country Analysis

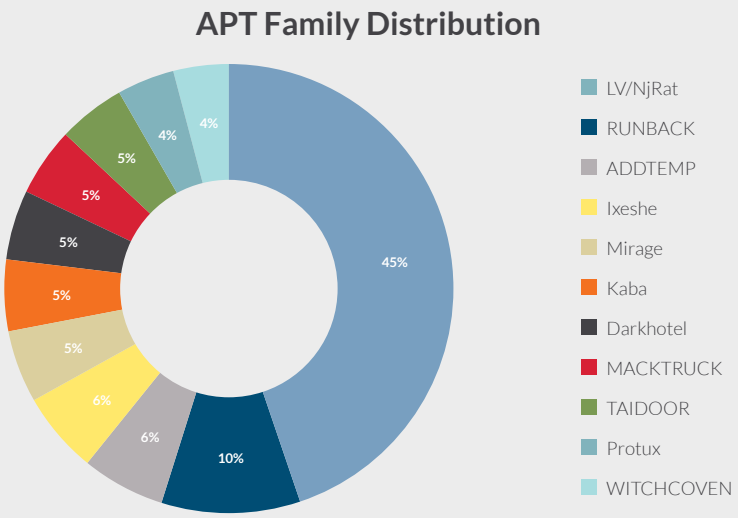
Israel, Saudi Arabia, Spain, Germany and the UK are the most targeted countries in EMEA.

Figure 2:
APT Detection by Country

The highest number of APT malware detected in EMEA in first half of 2015, by country, can be summarized:

1. Israel (11%)
2. Saudi Arabia (11%)
3. Spain (10%)
4. Germany (10%)
5. United Kingdom (9%)
6. Italy (9%)
7. Denmark (6%)
8. Turkey (6%)
9. Norway (5%)
10. Russia (5%)

Figure 2:
APT Detection by Country



APT Malware Families

The following graph represents the distribution of targeted malware families identified during this report. 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.

Whilst LV / NjRat was the most voluminous of the tools often used by APT actors, across all vertical markets, when looking into each separate vertical industry other patterns of preferred tool detection were discernable. FireEye constantly evaluate specific malware families and while we have observed LV / NjRat to be heavily used by cyber criminals, previous targeted attacks by suspected nation state threat actors have also utilized the same malware to conduct targeted attacks in the Middle East region.

Government, Finance, Aerospace and Energy are the top verticals in EMEA impacted by APT attacks

Vertical Analysis

Government, Aerospace & Defense Contractor, Energy/Utilities, Financial Services, Telecommunications were the most targeted verticals.

The following figure presents all malware activity, measured by number of unique alerts, by vertical for 1H2015. We have compared all malware and APT only events.

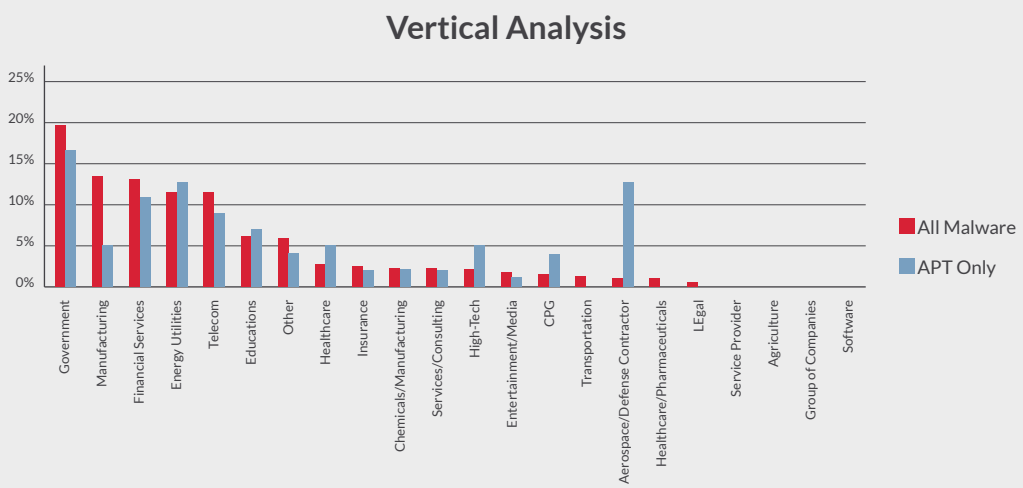
While most of verticals have very similar relative values of malware and APT only events, Energy/Utilities, Healthcare, High Tech, CPG and Aerospace & Defense Contractor have considerably higher volumes of APT.

On the other hand, Manufacturing has a much lower distribution of APT only events suggesting that they are impacted by mostly crimeware malware.

Additionally, Government, Aerospace & Defense Contractor, Financial Services and Telecom verticals represent more than 50% of total APT detections, and all are considered strategic industries in EMEA.

The following paragraphs provides an in depth analysis of the top three verticals impacted.

Figure 5:
APT Malware Detections per Vertical



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 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 generally testing their own skills or foreign government network defenses.

Organizations in EMEA are almost certain to face cyberespionage 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 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 employ cyberespionage capabilities to monitor their economic, political, and military interests, which will likely drive the further development of local cyberespionage 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.The most prevalent threat in the first half of 2015 within the government sector was.

Kaba (SOGU)

Whilst LV / NjRat was prevalent across all Vertical industry sectors, APT.Kaba is a preferred tool of many Chinese inferred APT groups and was the most prevalent tool in the Government sector across EMEA for the first half of the year.

Kaba is also known as:
APT.PlugX, APT.Plugx, Backdoor.APT.DestroyRat, Backdoor.APT.PlugX, Backdoor.APT.Plugx, FE_APT_plugx, Trojan.APT.PlugX, Trojan.APT.Plugx, Backdoor.APT.SOGU, FE_APT_Choiceguard_Kaba, FE_APT_DestroyRAT, FE_APT_Greedy_sogu, Trojan.APT.DestroyRAT.DNS

It is a backdoor primarily used by advanced persistent threat (APT) actors.

The malware is a backdoor capable of file upload and download, arbitrary process execution, file system and registry access, service configuration access, remote shell access, and implementing a custom VNC/RDP-like protocol to provide the command and control server with graphical access to the victim system's desktop. This backdoor provides threat actors with SQL database querying capabilities and communicates using HTTP POST requests or custom binary protocols. FireEye has observed threat actors deliver this backdoor through both strategic web compromises and phishing emails. Some phishing emails also dropped decoy documents onto the victim system along with this backdoor. This backdoor is frequently installed and launched by KORPLUG, a payload launcher that APT groups use.

FireEye currently attributes this backdoor activity to multiple China-based APT groups, to include APT9, APT10, APT17, APT20, APT22, APT26, and APT27. This backdoor is currently actively used by these threat groups.

NOTEABLE CASE IN GOVERNMENT: APT.RUNBACK

During the first half of this year, we detected a bloom of attacks targeting Turkish entities,APT. Runback has been discussed in the Open Sourceintelligence community as “Ghole”“rocket Kitten” and “Woolen Goldfish”. Attribution has been leveled at a Middle Eastern Country, and given the pivotal nature Turkey is playing in the current conflicts, intelligence gathering tactics would seem a plausible strategy for foreign vested parties. Interestingly APT.Runback uses TTPs commonly associated with CyberCrime threat actors, in that, a macro based decoy document acts as the lure, with the subsequent payload, being an off the shelf, licensable penetration testing tool.

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, asfinancial advisors are often at the heart of the mergers and acquisition process, this is a sensitive time for organizations 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 organizations 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 organizations, as well as information collection for possible foreign government scrutiny and insight.

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

THE MOST PREVALENT TOOL SEEN IN FINANCIAL SECTOR IS LV / NJRAT

This malware is a publicly available remote access tool (NjRAT) capable of keystroke logging, credential harvesting, reverse shell access, file uploads and downloads, and file and registry modifications.

This RAT also offers threat actors a "builder" feature, allowing them to create new variants based on configurations of command and control servers, specified filenames, options to spread via USB, designated campaign names for internal tracking, and other customization options.

Additionally, this RAT gathers and sends important information about infected machines to its command and control server, possibly using a custom protocol over port 80, to include NetBIOS name, user, date, locale, and Windows OS name. Traditionally, threat actors that deploy this RAT primarily use websites hosting EXE files to propagate the malware.

Since this malware is publicly available, a wide range of threat actors use this tool, but the RAT has become increasingly popular among Middle Eastern and African threat actors.

Middle Eastern threat actors have used this RAT to target a variety of industries, including Middle Eastern Governments, and telecommunications and energy industries, as well as frequently use this malware in cybercrime operations. FireEye has observed threat actors target our clients across multiple industries using this RAT, to include the energy, mining, food and beverage, manufacturing, and pharmaceuticals and biotechnology industries.

There are many groups using NjRat variants, and they exemplify the blurring of the lines motivations in the pursuit establishing unauthorized access in corporate networks, some groups have been attributed to nation state regimes, some groups are clearly patriotic, some have blatant criminal motivation and some display hacktivist motivation, many groups display a bit of everything, LV and the other versions of NjRat, have created an aftermarket bazaar for the resale or exchange of victims, this in itself has created demand and value in LV infections, and may explain why LV / NjRat is the most widely used tool, as trading in victims has become a commodity or a currency in its own right, it has also meant that in many cases, the threat actor infecting you, has absolutely no interest in your data, but, the person they sell you to, does.

ENERGY/UTILITIES

The energy and utilities industries are high priority targets for cyber threat actors, principally because of the continued advances in technology enabling the discovery and development of new or previously inaccessible energy sources. At the same time, oil prices have remained depressed after their fall in the past two quarters. Production by the world's top producers continues unabated, meaning that prices will continue to hold steady through 2015, contributing to the longest period of oversupply since the late 1990s. We observed that almost 50% of advanced threats in Saudi Arabia were targeted towards the Energy/Utilities vertical.

Additionally, SpyNet&GhOstRat were used in 30% of the observed possible infections across EMEA.

FOCUS ON SAUDI ARABIA

FireEye sees a continuing trend of advanced attacks against organizations in the Kingdom of Saudi Arabia ("KSA"). Education, which is always an easy target due to the liberal use of systems and resources for students to learn, allows attackers a perfect 'staging' environment, where they can have control of a system to launch a secondary (and more important) attack which was typically their ultimate goal. FireEye continues to build relationships with education institutes in the Kingdom to ensure cyber defense monitoring is on the top of their agenda. We see a very common use of Remote Access Tools (RAT) that is commonly employed across KSA education institutes to gain this initial footing. Most commonly detected by FireEye was the backdoor.APT.LV. What is interesting here is that the confidence of the attackers are very high using such a publicly known tool. When a tool is well known, it is supposed to be easy for an install Anti-Virus to find it. We see the high levels detected reflecting the easy at which the actor is employing a common tool knowing that a foothold is almost guaranteed. We need to make sure that institutes build defenses and not be this easy access to launch potentially larger more dangerous campaigns in the Kingdom and outside. FireEye has seen a steady increase in the use of Backdoor.APT.LV since the start of 2015. Utilities and Energy were continuously targeted, but not by such a commonly available tool such as the Backdoor.APT.LV malware; In the Energy and Utilities industry, we seem more of a focus I'm using advanced tools such as XtremeRAT and SpyNet. These tools, while publicly available, are not open for use, as they are more typically made available as a commercial tool. The XtremeRAT is also popular among attackers based in the Middle East, commonly seen in attacks by certain actors and also believed to be in use by the Syrian government.

AEROSPACE/DEFENSE INDUSTRY

FireEye believes that organizations in the aerospace and defense industry face cybersecurity risks from threat actors affiliated with a nation state and motivated by military or economic interests.

Nation state threat actors will likely target aerospace and defense organizations and attempt to steal intellectual property and proprietary information capable of providing their government with a military advantage. A benefitting government would likely be able to use stolen blueprints and other data to indigenously develop other nations' products. We suggest that this would allow states limited by security restrictions and other export controls to obtain technologies that they are not able to otherwise purchase.

Similarly, a government competing in the global arms market might use threat actors to steal information that would allow the country to indigenously develop and then sell new and highly valued technologies. Governments that engage in such activity would likely have an economic advantage in the market, as using stolen blueprints would allow them to skip the research and development process, and thus sell the products more cheaply.

Lastly, nation state threat actors may also attempt to compromise organizations in the aerospace and defense industry in order to damage or disrupt the function of critical technologies and systems. Conducting Computer Network Operations (CNO) against an adversary's systems during war would likely deny that adversary the use of the affected systems, potentially providing the perpetrator with a military advantage.

APT.NS01 ALSO KNOWN AS MUTTER

PLA unit 61398 attributed tools were also most notable in the Aerospace/Defense industrial Base, across EMEA. These tools have been linked toattacks from as far back to Operation Beebus through the C&C infrastructure along with the similar targets and timeline observed. Although some of the targets of these attacks overlapped with Beebus targets, there were many new targets discovered. As we uncover more targets related to these attacks, we are seeing a common link between them: unmanned vehicles, also known as "drones". The set of targets cover all aspects of unmanned vehicles, land, air, and sea, from research to design to manufacturing of the vehicles and their various subsystems. Other related malware have been discovered through the same C&C infrastructure that have a similar set of targets, that when included bring the total number of targets to more than 20 as of this writing. These targets include some in academia which have received military funding for their research projects relating to unmanned vehicles.

The tool detected as APT.NS01, also known as MUTTER is a HTTP proxy aware, and attempts to determine if a proxy is required and what the proxy details are if necessary.

This malware employs several interesting evasion techniques. For starters, it employs several "hide in plain sight" techniques common to malware used in targeted attacks. Firstly, It specifies fake properties, pretending to be Google or Microsoft and secondly. It's a whopping 41 megabytes. With rare exception, malware typically have a small size usually no larger than a few hundred kilobytes. When an investigator comes across a file megabytes in size, he may be discouraged from taking a closer look. Interestingly, the original size of this particular DLL is around 160 kilobytes, although the PE headers already indicate its future size as shown below. The dropper will decode this DLL from its resource section, drop it onto the victim's system, and proceed to fill its resource section with randomly generated data. This has another useful side effect of giving each DLL a unique hash, making it more difficult to identify.

CONCLUSION AND RECOMMENDATIONS

The evidence highlighted in this report demonstrates that organizations in EMEA are 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 organizations 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 your organization 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.
6. Its not the breach that will cause a Cyber Black Swan event, it's how you deal with it.

Credit to Yogi Chandiramani, Jens Monrad and Andy Norton for developing and anaylsing the data for this report

To learn more about
how FireEye can help you focus
on the alerts that matter,

visit:
http://www.**fireeye.com**

FireEye

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**