

SECURITY RESPONSE

Targeted Attacks Against the Energy Sector

Candid Wueest

Version 1.0 – January 13, 2014, 14:00 GMT

“ *The energy sector has become a major focus for targeted attacks and is now among the top five most targeted sectors worldwide.* ”

CONTENTS

OVERVIEW	3
Introduction	5
Exposed systems: Online and offline.....	7
Smart grid: A new potential avenue of attack	8
History of discovered attacks	10
2013	10
2008	10
2003	10
2001	10
2000	10
Stuxnet	11
Night Dragon	11
Shamoon/Distrack	12
Spear phishing attacks in the energy sector	14
New Year's campaign	14
Greek oil campaign.....	14
Motivation and origin.....	16
Protection and mitigation	16
Conclusion.....	19
Appendix	21
A. Spear phishing	21
B. Visualization with TRIAGE.....	24
C. Phases of targeted attacks	25
Resources.....	28

OVERVIEW

The energy sector has become a major focus for targeted attacks and is now among the top five most targeted sectors worldwide. Companies in the sector are facing a growing risk of having their services interrupted or losing data. The threat to energy firms is only likely to increase in the coming years as new developments, such as further extensions of smart grids and smart metering expose more infrastructure to the Internet. Equipment that is not connected to the Internet and other networks is not immune to threats and there has already been a number of successful attacks against isolated systems. Operators of critical infrastructure, as well as energy utility companies, need to be aware of these threats and prepare accordingly.

The threat to energy firms comes from several different sources. In some cases, espionage from competitors is the primary motive, with data on new projects, exploration and finances being targeted. Disruption and destruction are the goals of other attacks. Some instances appear to be state sponsored, such as the disruption of the Iranian nuclear program by the Stuxnet worm in 2010, one of the attacks that began this trend. Others appear to be the work of hacktivists with political or environmental agendas. Internal attackers, like disgruntled employees, are also a major source of attacks that often lead to service disruption. The majority of the actors behind these attacks have grown more sophisticated in the way they attack.

During the monitoring period from July 2012 to June 2013, we observed an average of 74 targeted attacks per day globally. Of these, nine attacks per day targeted the energy sector. Accounting for 16.3 percent of all attacks, the energy sector was the second most targeted vertical in the last six months of 2012, with only the government/public sector exceeding it with 25.4 percent of all attacks. The high ranking was mainly due to a major attack against a global oil company, which we observed in September 2012. However, in the first half of 2013 the energy sector continued to attract a high proportion of attacks, ranking in fifth place with 7.6 percent of targeted attacks.

Not all of the attacks analyzed used highly sophisticated tools. Most of them could have been prevented by following best practice guidelines for protecting the IT infrastructure and the industrial components, indicating that despite high revenues and strategic importance, many energy sector companies are not prioritizing cybersecurity.

INTRODUCTION

“Many power utilities companies fear disruptive attacks the most, regardless of whether it is done by internal or external attackers.”

Introduction

The number of targeted cyberattacks in general has risen in the past few years. In addition to this, the rate of attack exposure has also risen, with more companies becoming aware of attacks, expecting them and searching for indications of compromise. It is not a new phenomenon, but its importance has grown. The Council on Foreign Relations, a US think tank, reported that energy companies, including oil and gas producers, were often the focus of targeted attacks during summer 2012. In May 2013 the US Department of Homeland Security (DHS) warned of an increase in sabotage attacks against US energy companies located in the Middle East. The government had tracked multiple attacks and issued a warning together with the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). A report by the US Congress supported this picture, stating that many power utilities companies were under constant or daily attack through cyberspace. Taking into account that successful breaches of critical infrastructures are still rare and that these numbers included generic malware infections, it nevertheless highlights the potential for cyberattacks in the energy sector.

As in most sectors, attackers are often after valuable information. For example, we have seen attackers target intellectual property such as technology for photovoltaic research and wind turbines, or data on gas field exploration. Information such as this is of high value and can generate huge profits for attackers or their sponsors. The same information can also be misused for an act of sabotage. Many power utilities companies fear disruptive attacks the most, regardless of whether it is done by internal or external attackers. The energy sector has a high potential for critical disruption through sabotage attacks. Any interruption to the power grid would cause substantial chaos and cascading effects resulting in financial loss.

In the past there have been quite a few attacks that included targets in the energy sector. Some of these were more focused, like [Stuxnet](#), [Duqu](#), [Shamoon/Disttrack](#) and [Night Dragon](#). Others saw power companies targeted among many other sectors, such as [Hidden Lynx](#), [Nitro](#), [Flamer](#), [Net Traveler](#) and [Elderwood](#) to name a few. One of the biggest examples, and a game changer for many organizations, was Stuxnet. This targeted sabotage attack, which is believed to have been aimed against uranium enrichment facilities in Iran, made clear what could be done through cyberattacks.

It is also clear that the energy sector is not exempt from the generic attacks that every company faces, such as ransomware that locks PCs or financial Trojans that attempt to steal passwords and credit card details. For example, such a case happened in May 2013, when a small fuel distribution company in North Carolina fell victim to a [cyberheist that transferred US\\$800,000 from the company's bank account](#). Such threats spread broadly and might impact any person, regardless of their employer. These attackers aim at infecting as many computers as possible in order to maximize their chances of profits. These attacks can include nonspecific data breaches where employee or customer records get stolen, as happened to the US Department of Energy in July 2013.

For this paper we focused on email data from targeted attacks between July 2012 and June 2013. Even though watering holes are becoming more frequently used in targeted attacks, it is unfortunately quite difficult to reliably map these to individual campaigns. A blocked drive-by download attempt does not give any indication if it was a targeted attack or just general noise. In quite a few cases we see the same common malware, like Poison Ivy, being used by generic attackers and by targeted attacks. In such cases the sole difference between a sophisticated targeted attack and a generic one lies in the person commanding the malware.

EXPOSED SYSTEMS: ONLINE AND OFFLINE

“ Experts predict that billions of smart meters and sensors will be installed worldwide over the next ten years. ”

Exposed systems: Online and offline

Historically most industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems were in separated networks not connected to the Internet or any other network. Unfortunately this security through segregation approach does not fully protect against cyberattacks. In reality, networks are rarely completely isolated. Often some configuration updates are periodically installed or log files are transferred. If systems are not directly connected, the method of choice for these types of interactions is usually through a USB stick or a non-permanent modem connection, which provides a way into the restricted networks. This allows malware to spread into such isolated networks as demonstrated many times by threats such as Stuxnet.

If networks are truly segregated, this would mean that there would be no software updates installed, leaving old vulnerabilities open. There are also issues around processes. For example, the revocation lists for digital certificates are seldom updated and therefore certificates which are no longer valid cannot be checked properly and would still be accepted.

With the increasing desire for connectivity now reaching industrial plants, many operators have started to connect their ICS to the Internet. New adapters can bridge to older technology which was never intended to be controlled over the Internet, allowing it to be connected easily. This allows for efficient centralized monitoring and, to some extent, remote control of equipment.

Depending on the type of machinery controlled through the human-machine interface (HMI) of the ICS, not all modifications are possible. Some systems are physically connected in a pure read-only mode for monitoring. And even if they are fully connected, some turbines have physical limitations or emergency systems based on physical effects that cannot be overridden by the digital controller. Thus, not all Hollywood scenarios of open flood gates or turbines that fly through the air are possible. However, sabotage attacks that damage equipment are definitely possible, as has already been demonstrated. In the future, more systems are going to implement the failsafe switches in software, opening up the vector for malware attacks.

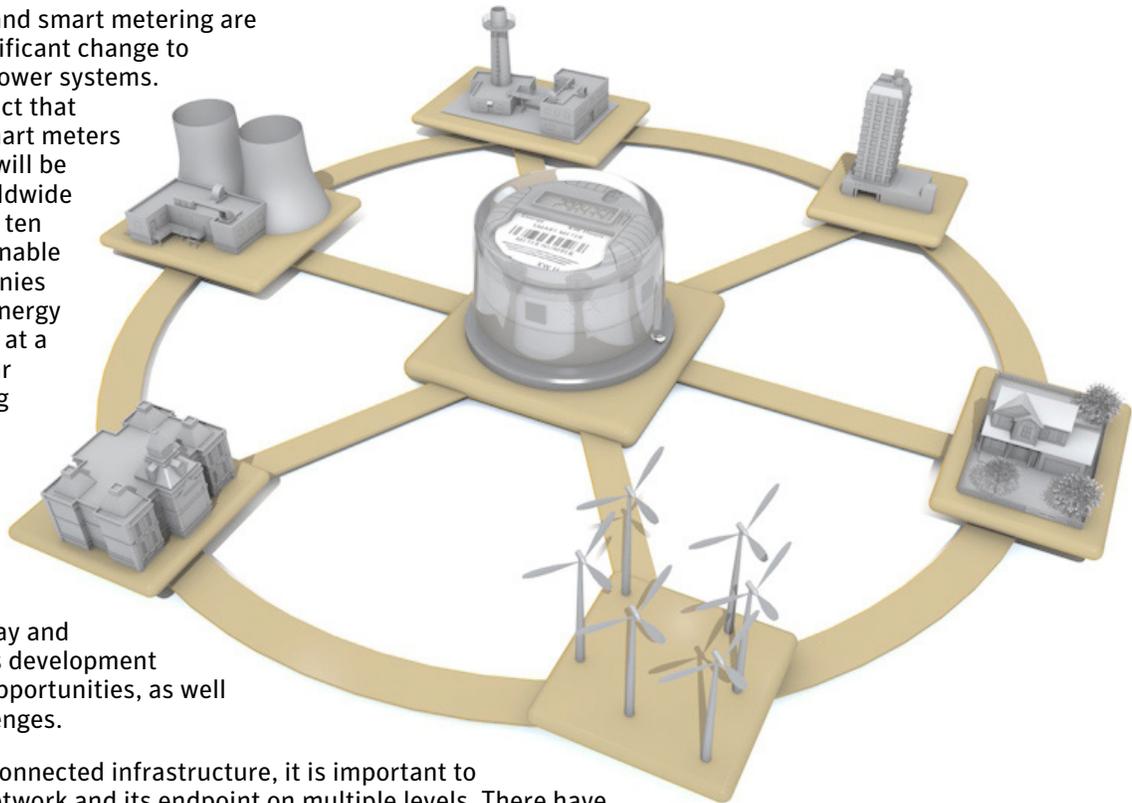
An additional source of concern is that some countries have started to open the energy market for smaller private contributors. This means that almost anyone can use mini power plants like water, wind or photovoltaic sites to feed energy back into the power grid. Often these operators do not have a full IT staff supporting the facilities at hand, which might lead to more vulnerable installations. Furthermore they may deploy new technology which might be untested and contain some unknown vulnerabilities. While these smaller sites make up only a small portion of the grid, new decentralized power input feeds are a challenge for the balance of the power grid as well and need to be carefully monitored. Small outages or changes can have a domino effect for the whole power grid.

To increase the exposure of energy firms even further, sites like [SHODAN](#), which is essentially a search engine for devices, enable anyone to easily find exposed controllers on the Internet. Of course not all of the industrial control systems connected to the Internet are critical systems or even real ones. Some researchers have started to create honey pot systems in order to study the attackers, which have apparently already attracted attackers like the Comment Crew/APT1 group, who have broken into these decoy systems.

Smart grid: A new potential avenue of attack

Smart grids and smart metering are bringing significant change to the world's power systems.

Experts predict that billions of smart meters and sensors will be installed worldwide over the next ten years. They enable utility companies to measure energy consumption at a more granular level, creating better flow patterns and enabling different prices for consumption based on the time of day and location. This development brings new opportunities, as well as new challenges.



As with any connected infrastructure, it is important to secure the network and its endpoint on multiple levels. There have already been proof of concept attacks that demonstrate how smart meters could be manipulated to send back false information or report incorrect billing IDs, leading to power theft.

In addition to the issue of securing these devices, smart grids will produce a huge amount of data which, depending on regulations, will need to be kept for audits. Some of this data may be sensitive and could raise privacy concerns if not properly protected. This could easily grow to petabytes of data that needs to be safely stored and managed.

It is beyond the scope of this paper to address all the challenges associated with smart grids and smart meters. Symantec has created a dedicated whitepaper for this topic: [How to protect critical infrastructure, mitigate fraud and guarantee privacy](#). As a member of the CRISALIS project, Symantec is following these developments closely and is helping to secure critical infrastructure together with partners from academia and different industry sectors.

HISTORY OF DISCOVERED ATTACKS



“ There have been numerous cyberattacks against the energy sector over the past few years. ”

History of discovered attacks

There have been numerous cyberattacks against the energy sector over the past few years. Not all of them were the work of sophisticated attackers; some incidents were just collateral damage caused by malware infections or bad configuration issues. These incidents highlight the fact that such attacks can happen and that they can have real life consequences.

2013

In 2013 part of the Austrian and German power grid nearly broke down after a control command was accidentally misdirected. It is believed that a status request command packet, which was broadcast from a German gas company as a test for their newly installed network branch, found its way into the systems of the Austrian energy power control and monitoring network. Once there, the message generated thousands of reply messages, which generated even more data packages, which in turn flooded the control network. To stop this self-inflicted DDoS attack, part of the monitoring and control network had to be isolated and disconnected. Fortunately the situation was resolved without any power outages.

2008

In 2008, Tom Donahue, a senior Central Intelligence Agency (CIA) official told a meeting of utility company representatives that cyberattacks had taken out power equipment in multiple cities outside the United States. In some cases the attacker tried to extort money from the energy companies, threatening them with further blackouts.

2003

In 2003 the safety monitoring system of the Ohio nuclear power plant apparently went offline for several hours due to a Slammer worm infection. Fortunately the power plant was already offline due to maintenance and the installed secondary backup monitoring system was unaffected by the worm. Nevertheless the incident raised safety concerns.

At the beginning of 2003 a marine terminal in Venezuela was targeted by a sabotage attack. Details of this attack are scarce and vague, but it seems that during a strike an attacking group managed to get access to the SCADA network of the oil tanker loading machinery and overwrote programmable logic controllers (PLCs) with an empty program module. This halted machinery, preventing oil tankers from loading for eight hours until the unaffected backup code was reinstalled on the PLCs. The attack was not too sophisticated as it was easily spotted. A small modification of the PLC code instead would probably have gone unnoticed for a long time.

2001

In 2001 an attack took place against California's power distribution center, which controls the flow of electricity across California. Due to apparently poor security configuration, the attacker was able to compromise two Web servers that were part of a developer network and penetrate further from there. Fortunately the attackers were stopped before they managed to attack any systems which were tied into the transmission grid for the Western United States.

2000

According to Russian officials, the largest natural gas extraction company in the country was successfully attacked in 2000. The attackers used a Trojan to gain access to the control for the gas pipelines. Through this switchboard, the flow for individual gas pipelines could have been modified, which would easily have caused widespread disruption.

Aside from these incidents, there have also been a number of more serious and well-documented targeted attacks against the energy sector:

Stuxnet

The Stuxnet incident and its relatives Duqu, Flamer and Gauss are some of the most talked-about cases of targeted attacks. As far as we know today, the Stuxnet operation began in November 2005 with the registration of the command and control (C&C) servers used in the attacks. The first recorded appearance of what we now call Stuxnet version 0.5 was in November 2007. Since then, a handful of different versions have been found and analyzed. Stuxnet 1.x is based on what is now known as the “tilded” platform; whereas Stuxnet 0.5 is based on the Flamer framework. The code segments and programming style differ, which indicates that two different programming teams were most likely responsible for the different branches of Stuxnet. Thorough investigation into the mechanism and functions of this threat started in July 2010. Stuxnet is the first known autonomous threat to target and sabotage industrial control systems to such an extent.

Stuxnet is a sophisticated piece of malware, which uses seven vulnerabilities to spread and infect its targets. The most notable vulnerability is the [Microsoft Windows Shortcut ‘LNK/PIF’ Files Automatic File Execution Vulnerability](#) (CVE-2010-2568), which allows it to auto-execute on USB drives. Spreading through infected portable media drives allowed it to also infect networks isolated by air gaps that are unreachable from the Internet. This was most likely the first infection vector used by Stuxnet. In addition, it is able to infect Step7 project files, which are used to control Programmable Logic Controllers (PLCs). This allowed the worm to infect computers whenever the engineer exchanged the project files. Besides this, it also spread through network shares, a printer spooler vulnerability, an old Windows RPC (remote procedure calls) vulnerability and a known password in the WinCC database. In the end, Stuxnet propagated further than its authors probably intended. We have monitored more than 40,000 infected IP addresses in 155 countries. Many of those systems are most likely just collateral damage and were not intended to be infected by the attackers. For example multiple computers at Chevron were infected by Stuxnet, without any damage being done.

Part of the malware code was signed with stolen digital certificates making it harder to detect by security tools. To hide its activity even further, Stuxnet executed slightly different infection routines depending on the security software installed on the target. On the USB drive itself, the malware would hide its own files and even delete itself from it after three successful propagations. Tricks like these, to make the detection of the malware more difficult, are now frequently used in modern targeted attacks.

Stuxnet’s payload focused on PLCs, which are used to control different industrial components. The target of the Stuxnet operation is believed to be a uranium enrichment facility in Iran. The sabotage payload disrupted and partially destroyed the cascaded high frequency gas centrifuges. The early version of Stuxnet targeted the S7-417 PLCs and modified its valve settings. Closing the valves at certain points in time would lead to an increase of pressure that could damage the equipment. The later version of the threat focused on the S7-315 PLCs, manipulating the spinning frequency of the rotating motors. By speeding the centrifuges up and slowing them down repeatedly, the output quality could be spoiled and the centrifuges themselves could be damaged. The payload would only become active if the fingerprint in the found PLC setup matched a given configuration setup. This minimized the collateral damage at other facilities and showed that the attackers had in-depth knowledge of the targeted uranium enrichment facilities. To avoid detection by personnel monitoring the human machine interface (HMI) of the plant, the threat recorded measurement readings during normal operation and played those back in a loop.

Night Dragon

Operation Night Dragon, which was uncovered in 2010, is a typical example of global oil companies being targeted, but this time not with the aim of disruption in mind. The attacks started in late 2009 and were directed at finding project details and financial information about oil and gas field exploration and bids.

The attackers started by compromising public facing Web servers through SQL injection and installing Web shells on them. Once they had control over the server they used common hacking tools to harvest local

passwords, dump password hashes, sniff authentication messages and exploit internal active directory configuration. This allowed them to move on to other internal computers using the gathered passwords. In addition, spear phishing messages were used to compromise additional computers. The attackers did not use any zero-day vulnerabilities during their attacks. Rather they used publicly available tools for each individual job.

On compromised computers a common [Backdoor.Trojan](#) was installed that communicated back to the C&C server, allowing remote access to the computer. This allowed the attacker to find and extract valuable information.

Shamoon/Distrack

In August 2012 an extremely destructive cyberattack hit an estimated 30,000 computers at one of the largest oil producers of the world in Saudi Arabia. The [W32.Distrack](#) malware used in this attack, also known as Shamoon, consists of three components: a dropper, a wiper and a reporter module.

The dropper component is responsible for creating all the required files on the system, registering a service called "TrkSvr" in order to start itself with Windows. It also attempts to copy itself to accessible network shares and execute itself remotely if successfully copied.

The wiper component is only activated when a hardcoded configuration date has been passed. This enables a coordinated, "time bomb" scenario. The module then drops a legitimate and digitally signed device driver that provides low level disk access from user space. The malware collects file names and starts overwriting them with a JPEG image or 192KB blocks of random data. At the end Distrack finishes the computer off by wiping the master boot record with the same data.

The reporter component is responsible for sending back a HTTP GET request to the C&C server. It reports the domain name, IP address and number of files overwritten.

By acquiring user credentials and gaining access to the domain controller the attackers were able to push the malware on to many systems before they triggered the destructive payload. Distrack's secondary goal may have been to steal valuable information from infected computers, but the main intent was to render the computers unusable by wiping the operating system and master boot record, causing disruption and downtime at the targeted company. Although wiping is also frequently used to destroy evidence of the attack and make forensics more difficult. The malware does not contain any payload against ICS, like Stuxnet does for PLCs, and is not as sophisticated. According to the company, no computer related with the production or distribution of oil was affected, since the operational network is separated and specially protected.

One group that claimed responsibility for the attack posted on Pastebin that it was an anti-oppression hacker group. The attack was prompted by disappointment with some of the regimes in the Middle East, the group said. True or not, this shows that it is not necessarily only state-sponsored attackers who are carrying out disruptive attacks. Sabotage attacks usually fall into the orbit of hacktivists, who seek attention rather than profit. Some sources reported that the attackers had help from insiders, which would explain the so far unclear infection vector.

Soon after this attack became known, a Qatari gas company was attacked in a similar way.

SPEAR PHISHING ATTACKS IN THE ENERGY SECTOR

“ A spear phishing attack consists of an email with either a malicious attachment or a link to a malicious website.

”

Spear phishing attacks in the energy sector

Spear phishing is, along with watering hole attacks, one of the most common attack vectors used to attack companies. The attacks are simple to carry out. They often follow the same pattern, starting with a reconnaissance phase to gather all publicly available information. This is followed by the incursion phase of breaking in and compromising computers. After that comes the discovery phase, where the attacker gathers passwords and maps the internal network. The final stage is capture and exfiltration, where the valuable information is copied and sent back to the attacker. The last phase may also involve a disruption attack if the goal is sabotage. For a more detailed analysis of the attack phases, see Appendix C.

A spear phishing attack consists of an email with either a malicious attachment or a link to a malicious website. Such emails are sent in bulk to a handful of key users. These waves are often repeated till enough people fall for the bait and compromise their computers. For analysis on the social engineering themes used, attack details and attachment types used, see Appendix A.

New Year's campaign

Some of the spear phishing campaigns are smaller in scale and are focused on specific targets. For example, on January 1, 2013 a global energy research company was targeted.

A wave of spear phishing emails were sent from two Freemailer accounts to 291 individuals at the targeted company. All receiving email addresses started with a letter between G and R, covering half of the alphabet. Whether there was a second wave of emails using the other half of the alphabet or whether the attackers only got their hands on part of the address book remains unknown.

All emails had either the subject line "2013,Obama QE4! Merry Christmas !" or "2013,Obama QE4!". It is common to see spear phishing attacks take place around holidays, as people are receiving more emails during these times and are less likely to perform due diligence while opening them. All of the emails contained the same [Trojan.Dropper](#) disguised as an attachment with the filename AVP.dll.

The malware itself drops a malicious Downloader "clbcatq.dll" into a newly created "wuauct" directory, posing as Windows update and taking advantage of the DLL search order hijack weakness in order to load the malicious code in Windows. The same family of dropper has been used in previous targeted attacks against other sectors, indicating that a group with multiple interests is behind the attacks. The back door provided full access to the compromised computers.

A week later, on January 7, 2013, the group attacked the same company again. Seventy emails were sent to 58 individuals using either "2012-13 NFL Playoffs Schedule" or "Re: 2012-13 NFL Playoffs Schedule" as a subject line. In this wave, the attackers used a similar AVP.dll to the one used before. In some of the emails, an additional CHM file with an old exploit was used in an effort to maximize the chances of a successful infection.

After this second wave, the attack ceased. It is unknown if the attackers successfully retrieved the information they were seeking, if they installed other back door Trojans or gained passwords that allowed them to directly access the computers, or if they have given up on the target.

Greek oil campaign

A global oil company, with offices around the world, had been under continuous attack for some time, but in September 2012 we noticed an upsurge in activity, with 34 times more suspicious emails than on average. This provided a clear indication that something suspicious was going on. At the end of this wave of emails, a hotel chain, a rental car company and two financial institutions were also targeted by the same attacker. This may have been an attempt to find further information that could be used in a future social engineering attack against the oil company.

In total, 136 email accounts at the oil company were targeted. A regional sales manager in Greece received

412 emails over the 12 month period, with 155 different attachments. A HR person in the same country received the second largest amount of emails with 90 in total. Seventeen other people were targeted between 70 and 90 times, many in the same region. The rest of the targeted people received less than five emails each, in what seems to have been an undirected spraying in the hope that at least some would fall for the bait. Clearly the one person that received the highest volume of emails was deemed to be of high value to the attackers. Possible explanations for the attack could be that a competitor wanted to know more about some upcoming deal or details on the oil field exploration, but this would be highly speculative.

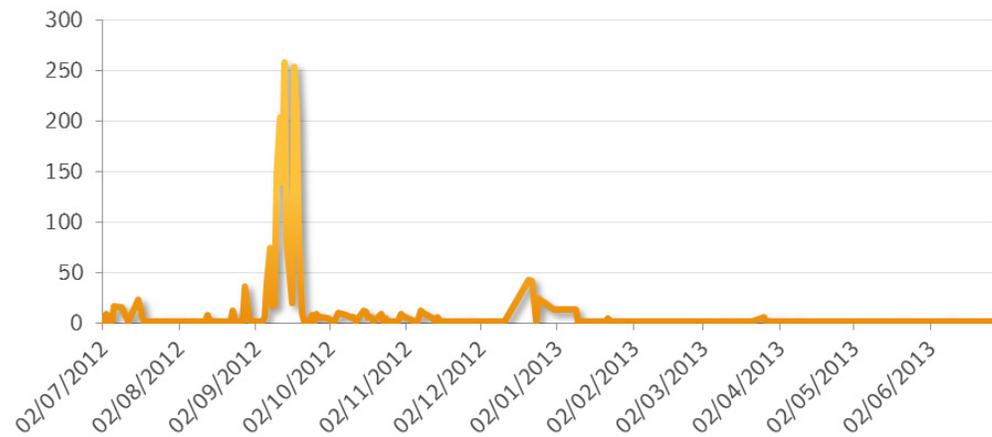


Figure 1. Number of emails targeting the company per day

The spear phishing emails came from 234 spoofed addresses. They were made to appear to be linked to the company in relation to the subject and attachment chosen. Many of the emails came from the same country as the main targeted sales manager.

The emails all contained malicious attachments. None of them linked to third party sites for drive-by downloads. Of the attachments, 1,588 had a .exe extension. Of those, 842 had a .pdf.exe extension. The malware chosen was a variant of the Poison Ivy Trojan [Backdoor.Darkmoon](#) and, in some minor cases, Trojan droppers that would download additional malware. The attackers did not use any zero-day exploits to drop a payload.

The social engineering messages concentrated mainly around the following two themes:

E-books and newspapers:

- E-Book.pdf.exe
- BusinessWeek.pdf.exe
- Financial Times E-Paper.pdf.exe
- The Economist Print Edition.pdf.exe
- The NY Times In Print.pdf.exe

Free desktop tools:

- Babylon9 - Greek.exe
- Google Desktop Translator.exe
- SMS Free Sender Desktop.exe
- BBC iPlayer.exe
- Sticky Notes Desktop.exe

Once installed, the back door would create a registry run key in order to restart with Windows and connect to one of three C&C servers located in Greece. The last C&C server has been used since 2010 in similar attacks against other companies. Other sub-domains at the same free host and DNS service have been used by other groups to spread malware in the past.

- updates.zyns.com
- amazaws.dyndns-office.com
- msupdate.3utilities.com

The chosen names of the C&C server domains imitates legitimate services in a bid to be overlooked by the system administrators when checking their logs.

The back door provides full remote access to the compromised computers, allowing for extraction of any data. It is unknown if the attackers succeeded in their goal and if valuable information has been extracted. The attacks did not completely disappear, but the email volume decreased significantly to only a few emails per week afterwards.

Motivation and origin

As with all targeted attacks, there are many different groups of attackers operating in this field. These attacks cannot be attributed to only one group or geographical region. We have seen individuals, competitors, hacktivist groups and possible state sponsored agents carrying out attacks against energy companies. Some of the attacks have been purely opportunistic, seeking any valuable information available. Other campaigns look like they were planned over a lengthy period and carried out methodically with a clear goal in mind.

The attackers tend to go after valuable information, including maps of new gas fields or research on efficient photovoltaic generators. This information can be of great value to competitors or nations that want to make progress in the same field. Another motivation for attackers is to profit from the information stolen by blackmailing the company.

The same information can be used to carry out sabotage attacks designed to disrupt ICSs, as the energy sector is also a primary target for sabotage attacks which will not generate direct profit for the attacker. A competitor might be interested in generating bad press and bad customer experience for a rival company, in order to win some new clients.

For example, in January 2013 a group claiming to be related to Anonymous [posted](#) access details for what they said were Israeli SCADA systems for power plants and other systems. Meanwhile, "[Operation Save the Arctic](#)" targeted multiple oil companies around the globe in protest against drilling plans in the Arctic.

Disgruntled employees are also a source of attacks that should not be underestimated. With their knowhow about internal critical processes and systems they often know how to inflict serious damage. They may be able to perform system modifications that could go unnoticed for a long periods.

Protection and mitigation

For all regular client computers, the well-established best practice guidelines apply. These computers are often the first ones to be attacked. Once compromised, the attacker will use these computers and try to explore deeper into internal networks. Securing and hardening of deployed operating systems with a working strategy for patch deployment is important. Reoccurring security awareness training can help users to identify social engineering attempts and prevent them from falling victim to them in the first place.

The company can perform penetration testing on Web and network applications but also on ICSs to identify and remedy any vulnerability. For examples Web applications should be tested against SQL injection attacks. This can also help confirm if applied policies are followed through, if the patch level is correct on all computers and if systems are compliant.

Companies can monitor the Internet for information about attacks in the same vertical and apply lessons learned where possible.

In addition, different layers of security products can help achieve better overall protection.

- **Security Information and Event Manager system (SIEM):** Using a SIEM can help correlate all related alerts in one place. This centralized view can be cross referenced with threat intelligence data to generate prioritization and an action plan. Painting the bigger picture of the overall security state can reveal previously unnoticed attacks. For example failed login attempts on internal servers could indicate a password breach. This includes logging of critical systems and synchronization of time among multiple systems.
- **Ingress and egress filtering:** Filtering the network traffic with firewalls, content filters and IPS allows the control of data flows. This can prevent attackers from reaching internal systems. It is important to also monitor outbound traffic, as data exfiltration is a key point for cyberespionage. It should be noted that with the increased use of cloud services and mobile devices, some traffic might never pass through the company's gateways. Where traffic blocking is too disruptive at least monitoring should be implemented.
- **Data loss prevention (DLP):** DLP solutions can track the access and flow of critical information and prevent it from leaving the company or encrypt it automatically.
- **Endpoint protection:** Depending on the usage pattern of the computer, different solutions are available to protect the endpoint. Antivirus solution with proactive detection methods like behavioral analysis and reputation scanning can prevent unknown malware from installing itself. HIPS (host based intrusion prevention systems), behavioral lockdown or whitelisting can protect computers from any kind of unwanted tampering without the need of constant updates.
- **System protection:** For non-standard IT systems, hardening can increase the security. On industrial systems which are not often updated or that cannot be updated, exploitation can be prevented with the help of lockdown solutions like Symantec Critical System Protection (CSP). Through policies, only trusted system applications are allowed to run. ICS should be regularly checked and upgraded if new firmware exists. Where this is not possible HIPS and behavioral lockdown tools can be used to secure computers.
- **Email filtering:** Proper email filtering can prevent many spear phishing attempts from reaching users. They can help minimize the risk of an untrained user falling for social engineering tricks.
- **Authentication:** Some of the ICS contain hardcoded passwords and, wherever possible, these should be changed. ICS frequently use weakly authenticated protocols that allow for impersonation attacks. Where possible those authentication methods should be upgraded or at least closely monitored. Strong authentication or PKI should be used where applicable.

Industrial control systems (ICS) should be specially protected and monitored. The control system and control network should be secured. Where possible, ICS should be separate from the Intranet. Isolating these networks alone is often not enough to protect the control network, but it can make it more difficult for attackers to succeed. For some systems it can make sense to have a plan to quickly disconnect or separate critical machines in the event of a detected cyberattack.

CONCLUSION

“ In the second half of 2012, the energy sector was the second most targeted with 16 percent of all the targeted attacks. ”

Conclusion

Cyberespionage campaigns and sabotage attacks are becoming increasingly common, with countless threat actors attempting to gain a foothold in some of the best protected organizations. At this stage, roughly five targeted attacks per day are being mounted on firms in the energy sector. These attacks have become increasingly sophisticated, although the capabilities and tactics used by these threat actors vary considerably.

In the second half of 2012, the energy sector was the second most targeted with 16 percent of all the targeted attacks. This strong increase was mainly due to a large scale attack against one global oil company. In the first half of 2013, the energy sector was ranked fifth with 7.6 percent of all attacks focused on this sector. In general we have observed that attackers are becoming more efficient and focusing on smaller operations that attract less attention.

The attackers tend to go after valuable information – such as maps of a new gas field – but the sector is also a major target for sabotage attacks, which will not generate direct profit for the attacker. Such disruptive attacks do already happen and may lead to large financial losses. State sponsored agents, competitors, internal attackers or hackers are the most likely authors of such sabotage attacks.

Fortunately, there have not been many successful sabotage attacks against energy companies to date. However, the increasing number of connected systems and centralized control for ICS systems means that the risk of attacks in the future will increase. Energy and utility companies need to be aware of these risks and plan accordingly to protect their valuable information as well as their ICS or SCADA networks.

APPENDIX

Appendix

A. Spear phishing

Social engineering themes used

Social engineering is an essential part of spear phishing campaigns. A cleverly chosen, enticing message may prompt the user into opening an attachment. It is evident that most attackers are carefully selecting the themes that they use for their attacks. Some groups use real news stories and copy the text directly from the newspaper websites. Others try to appeal to personal hobbies in order to get the user's attention.

In the energy sector the most commonly used theme for spear phishing emails was money related (e.g. "Wage Data 2012") followed by sports related themes (e.g. "2012-13 NFL Playoffs Schedule").

As an example, the subject line "Wage Data 2012" was used in 944 emails, sent from 26 different email addresses to targets in nine different sectors. The attack was carried out over eight days and used the same infected Microsoft Word document in every instance.

In general any topic can be used in a social engineering attempt, which makes it even harder for regular users to spot the attacks. Here are a few examples of subject lines used, listed by category:

Contact detail updates:

- Updated Corporate & Regional Office Contact Information
- Updated Information For Contact List
- Address Change

Event and conference details:

- The Energy and Economic Summit 2012
- 12th Annual International Conference on Politics & International
- Fw: Doha Climate Change Conference - November 2012
- US Energy Information Administration Invitation

Global news stories:

- BREAKING NEWS PHOTOS, BEIJING
- President Obamas Asia Policy and Upcoming Trip to the Region
- DoD Protection of Whistleblowing Spies
- U.S. Engagement in the Pacific

Money related:

- Acknowledge Payment
- Payroll Invoice for week ending 02/15/2013 - 09509
- Bank Details/Swift Code Error
- Unable to process your most recent Payment

Sport related:

- 2012 NFL Schedule
- 2012-13 NFL Playoffs Schedule
- 2012-08-02 Thursdays sixth day of the 2012 Olympic Games
- London 2012 Medal Top 10

Lifestyle related:

- 125 Best Foods for Men
- 2013 Lingerie Calendar... discover your deepest desires!

- 8 Minutes to a Longer Life

Special interest groups:

- Shamoon Upgrade Edition Malware Might Be Flame Copycat!
- CyberAlert: Cyberattacks spread in banks all over the world
- 3D printing technology used in Chinese fighter jets
- 2013 Defense Industries Manufacturing

Speare phishing attack details

In the last six month of 2012 the average number of targeted attacks observed per day was 87 (with 14 in the energy sector). In the first six month of 2013 the average number decreased to 60 targeted attacks per day (five in the energy sector). The spike in August and September 2012 is mostly related to a large scale attack against a global oil company. The increase in May 2013 was due to multiple attacks against financial services, public sector and IT service organizations.

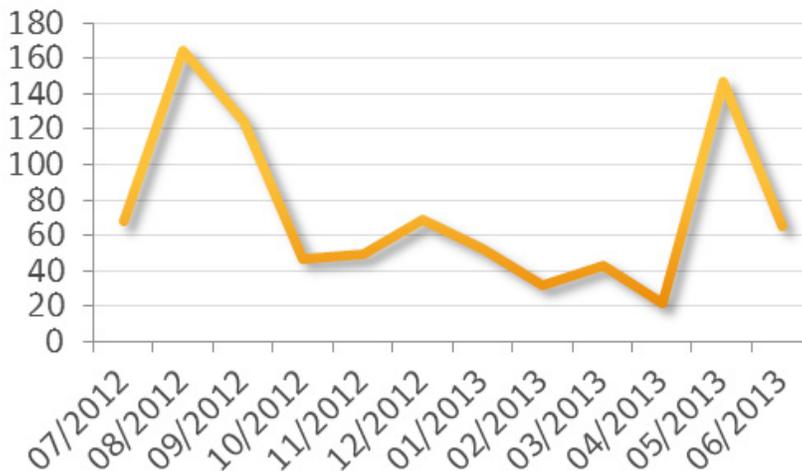


Figure 2: Number of targeted attacks per day

The government and public sector was quantitatively the most attacked sector, with 25.4 percent of all targeted attacks falling in this sector for the last half of 2012 and 24 percent for the first half of 2013. The energy sector accounted for 7.6 percent of all targeted attacks, making it

the fifth most targeted sector in the first six month of 2013. This was a big decrease from 16.3 percent of all attacks in the last half of 2012, when it was the second most attacked sector. This spike in 2012 is mainly due to a large attack campaign against a global oil company which took place in September 2012.

On average we saw 18.6 mail accounts being attacked for any given target company in the last half of 2012 (60.7 in the energy sector) and 5.6 email accounts in the first half of 2013 (10 in the energy sector). Overall, we see a trend of the attacker conducting more focused attacks against fewer individuals. This generates less noise and the risk of getting noticed or discovered is smaller. These emails are sent in small bursts and then

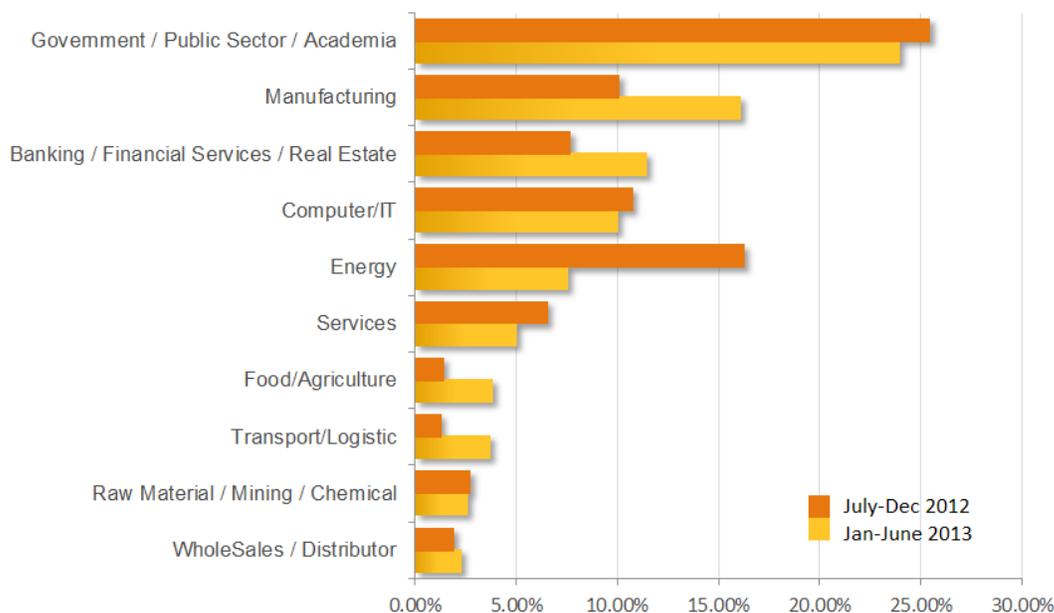


Figure 3: Top 10 of targeted attacks by vertical sectors

repeated against a changing target space till enough computers are compromised.

Attachment types used

Half of all the attachments analyzed used an extension that would run directly when double clicked. This old method is still the most common scheme used. Of all attachments analyzed, 38 percent were .exe and 12 percent were .src files. In total only 6 percent used double extensions like .pdf.exe to fool the user. It should also be noted that 23 percent were Microsoft Word documents using some exploit to execute custom code on the computer.

There were also some more exotic extensions used like Autolt scripts (.au3) and ZX-Edit files (.zed), but these are the exception rather than the rule. It might be that the attackers tried to bypass some email filtering software by experimenting with different attachment types. Sometimes even older exploits like the [Microsoft DirectX DirectShow Length Record Remote Code Execution Vulnerability \(CVE-2009-1539\)](#) in .mp4 files are still occasionally used. This indicates that either not all attackers have the knowhow to use newer exploits that are publicly available or they speculate that the target has not patched all computers. Some of the attackers do not seem to be too sophisticated. For example they used "www.[COMPANY-NAME].com.exe" as an attachment name, clearly missing that the ".com" at the end would be sufficient to run it and the additional ".exe" was not needed.

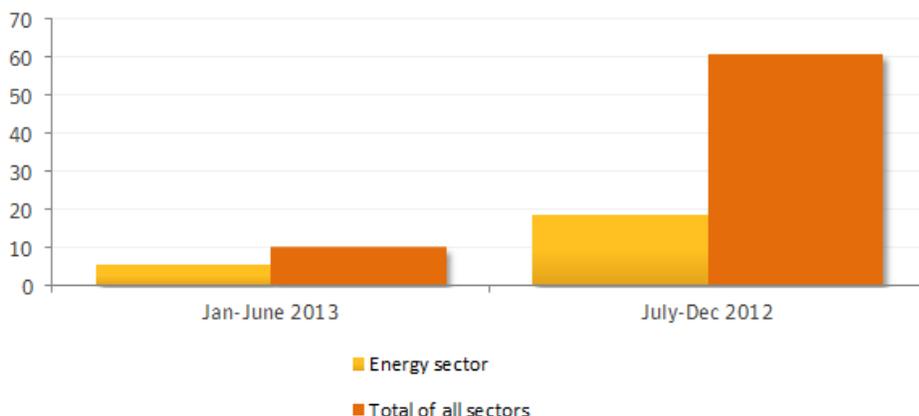


Figure 4: Average number of mail accounts targeted per company

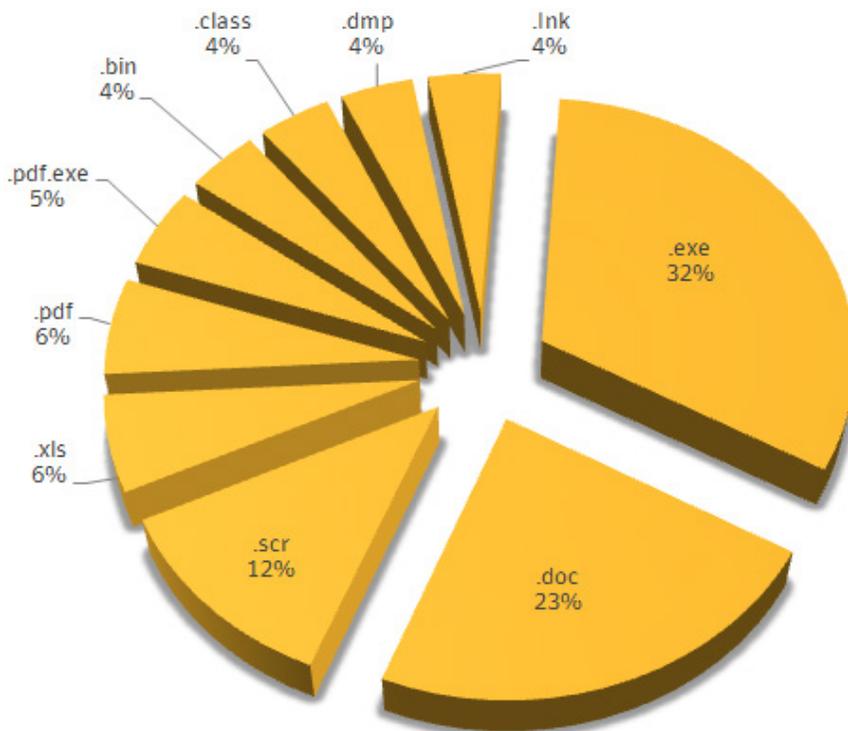


Figure 5: Extensions used in targeted attack emails

B. Visualization with TRIAGE

To identify a series of targeted attacks that are likely performed by the same individuals, we have used a novel attack attribution methodology named TRIAGE. Developed by [Symantec Research Labs](#), TRIAGE is data mining software that relies on multi-criteria decision analysis and intelligent data fusion algorithms to reliably link different attacks to the same source. This framework has been developed in order to automate cyberintelligence tasks and reduce the time needed to get insights into organized cybercrime activities. By enabling rapid analysis of large security data sets, Symantec analysts can then quickly and more efficiently attribute various waves of cyberattacks to a specific attack campaign likely run by the same individuals.

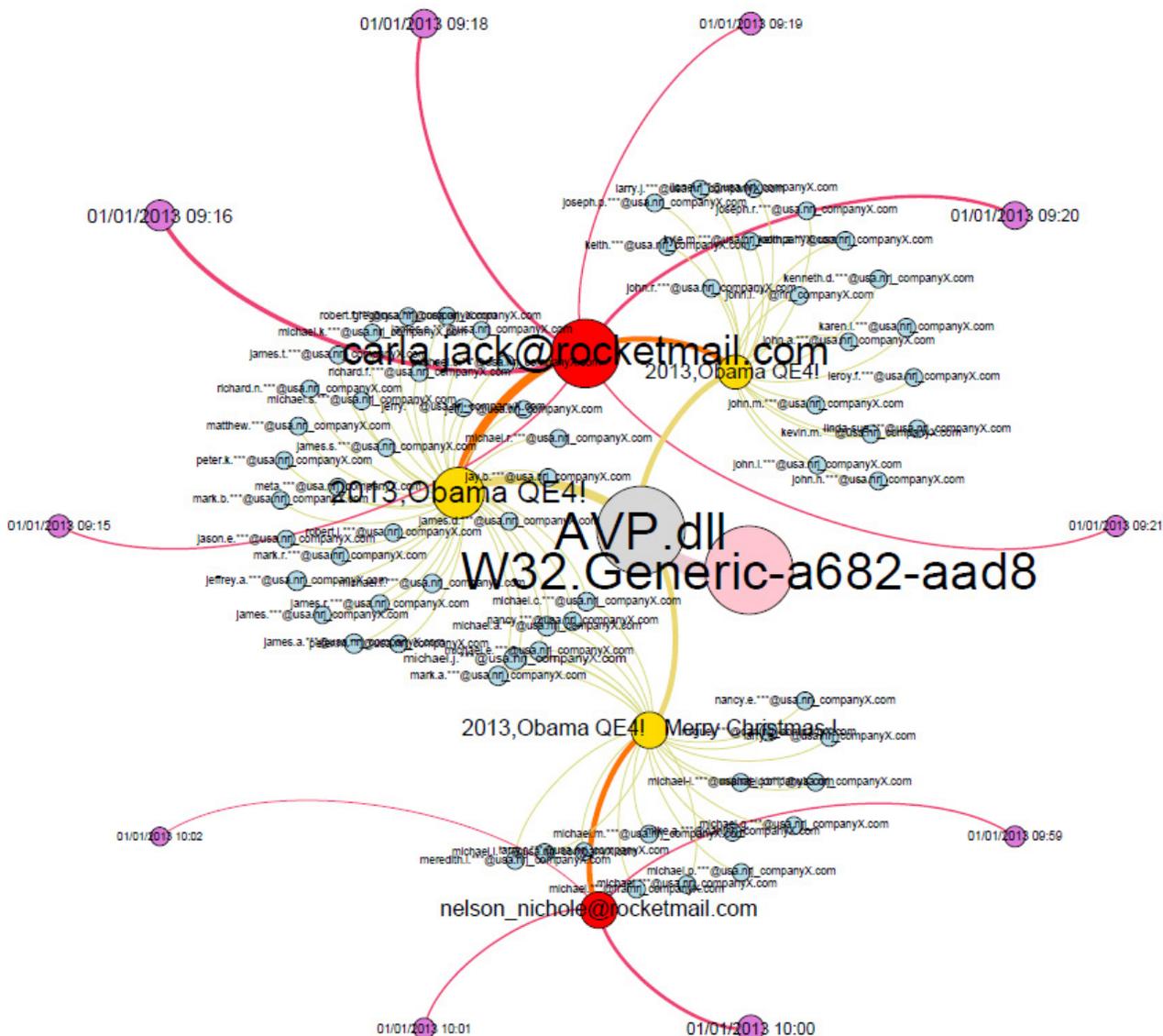


Figure 6: Graph view of attack wave against company targeted in the New Year's campaign

The TRIAGE framework was recently enhanced with novel visualizations thanks to [VIS-SENSE](#), a European research project aiming at developing visual analytics technologies for network security applications.

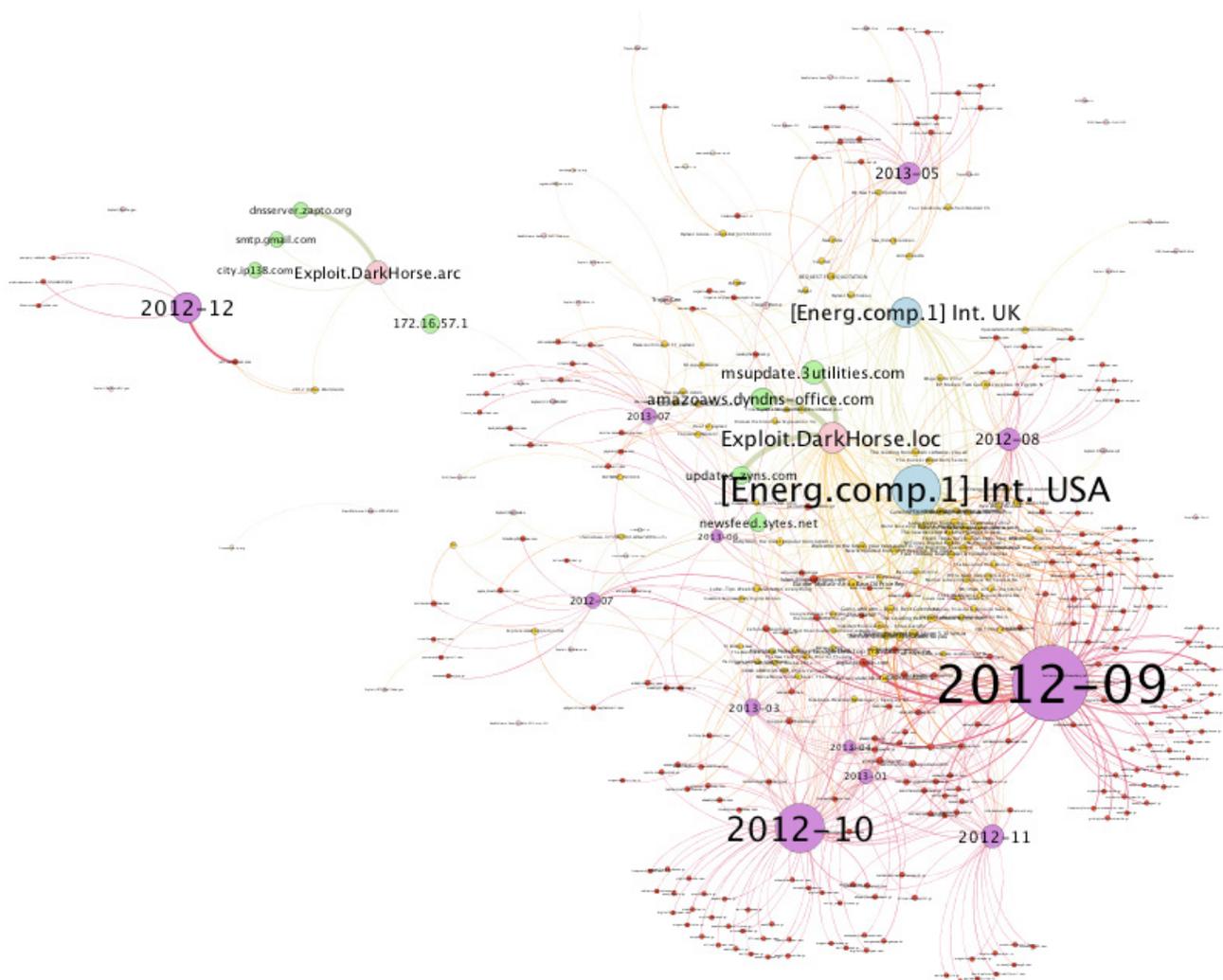


Figure 7: Visualization graph of the Greek oil campaign

Since its original conception, TRIAGE has been successfully used to analyze the behavior of cybercriminals involved in various types of Internet attack activities, such as rogue antivirus websites [1], spam botnets operations [2], scam campaigns [3] and targeted attacks performed via spear phishing emails [4,5].

C. Phases of targeted attacks

As with any other targeted attacks, attacks against the energy sector often follow the same pattern. It can be broken down in different phases of attack. It should be noted that we have seen attackers modify their behavior and exceptions from the norm and this is possible especially if the target company has special circumstances or security measures in place.

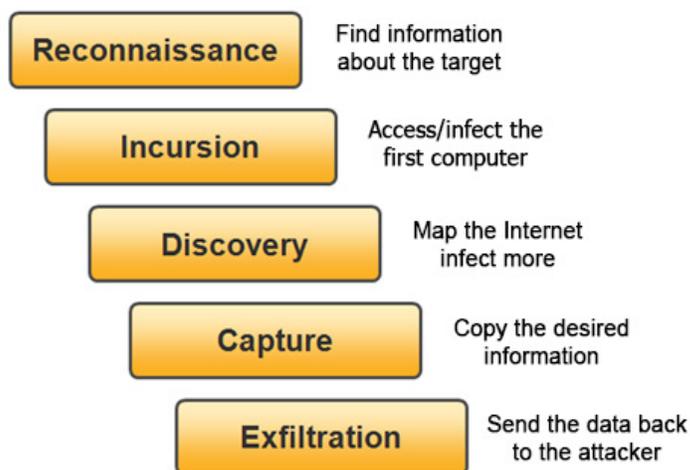


Figure 8: Typical phases of targeted attacks

Reconnaissance phase

During this phase the attacker tries to learn as much as possible about the targeted organization.

Information sources often include social networks, job posting sites and press releases. This enables the attacker to learn the contact details of possible target individuals as well as context that can be used in social engineering scenarios. The attacker will often create a list of implemented security software used at the targeted company from whatever information is available. These investigations often start completely passively without any direct contact with the company, since there are many data sources publicly available. Subsequently the attacker can use more interaction if needed. Some attackers go through all the effort of creating a fake social media account and befriending key employees. After a period of small talk, to create a false sense of security, such a connection can then be used to pass on an infected document or find out about some key information. Depending on the targeted location, physical reconnaissance and eavesdropping may also be used.

Incursion phase

The actual break-in occurs during this phase. The attacker usually compromises the network by delivering targeted malware to vulnerable systems or employees. There are two main avenues of attack. One is to send spear phishing emails, where a link to a malicious website or a malicious attachment is delivered using social engineering techniques. The second method, which is gaining traction, is watering hole attacks, where the attacker infects a website that has a high likelihood of being visited by the intended victim. By using IP address filters before infecting any visitor of such sites, the attacker can reduce the number of infected systems and bring it to a manageable quantity which can be assessed manually at another time.

Some groups carefully plan watering hole attacks. For example the [Hidden Lynx](#) group stopped using a zero-day vulnerability in a large watering hole attack after Microsoft released details on the vulnerability. This helped to cover their activities and avoid unwanted attention. A few days later the group resumed the watering hole attack again, this time using a different exploit.

For more difficult targets, man-in-the-middle attacks can be used. These can be performed either at the same physical location, posing as a genuine Wi-Fi hotspot or through supply chain attacks. This can enable the attacker to swap an update of legitimate software for a maliciously crafted version. Once the victim installs the genuine looking update, the attacker effectively gains control over the computer. Due to the complexity of such an attack, they are rarely used. Depending on the skills of the attacker and the time available, the attacker might also attack systems at the perimeter, such as Web servers, and try to break in from there.

The malware used is not always sophisticated. Sometimes a regular off-the-shelf back door Trojan is used. In these cases the person behind the malware orchestrating the commands is what makes the difference between a targeted attack and a broad generic infection. Having said this, on very unique targets, we will often see the use of a specifically designed piece malware, such as in the case of Stuxnet. Depending on the protection measures implemented by the target, the attackers may also digitally sign their malware creation. In the past there have been quite a few cases where code signing certificates were stolen and later misused to sign malware in order to pass it unnoticed to high value targets.

Discovery phase

Once the attacker has a foothold on one system, the next step is to create a plan for lateral movement through the network until the interesting data is found. With more specialized teams of attackers, we can often observe that the infected system is first analyzed to ensure that it is of interest to them. With watering hole attacks especially, it can happen that computers that were not targeted get infected. Infected computers need to be assessed by the attacker and, if necessary, removed to keep the profile, and with that the chances of exposure, low.

One of the obvious tasks performed by attackers is to install key loggers, dump local credentials, search local storage for saved accounts and sniff the network for passwords. Any account detail can be useful to them. Domain administrator passwords are of especially high value, as they can help greatly in moving further through the Intranet. Often small scripts or even manual commands are used to comb through local files and create network mappings. Simple system commands can help the attacker to learn about installed security tools, saved links to internal

platforms and local address books. Once new systems are identified the attacker will attempt to hop onto them as well. In some instances they might even use zero-day vulnerabilities to spread further into the network.

One method which is gaining more relevance is the hijacking of local software distribution systems for further distribution. This can either be proprietary systems, such as the case of [Trojan.Jokra](#) in South Korea, or OS-specific, such as hijacking Windows Update, in the case of Flamer. Once the attackers have successfully managed to create and distribute their own package, they can easily infect all connected systems at once. Especially in cases of wiping attacks, such Trojan.Jokra, this is a very efficient way to disrupt as many computers as possible.

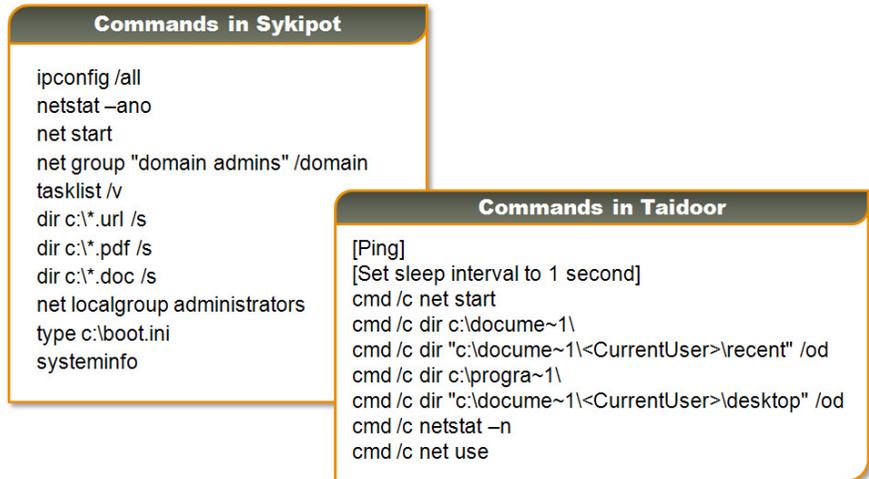


Figure 9: Typical commands used during discovery phase

If the target is assumed to be in a separated network not connected to the Internet, the malware used might try and autonomously infect removable drives, like USB sticks, or project files for PLCs. This could allow the malware to be manually introduced to the destination network, without the knowledge of the carrier, essentially jumping air gaps into isolated networks.

At the end of the discovery phase the attackers should know the internals of the infected networks and have identified systems with interesting data or with connected industrial control systems.

Capture/exfiltration phase

The capture and exfiltration phases are not always present. If the sole goal of the attackers is to cause a disruption they may directly jump to a destructive payload. However, in most cases information is extracted first, which in turn allows the sabotage to be constructed more efficiently at a later phase.

In this phase the interesting data is gathered and sent back to the attackers. This can be done with different levels of sophistication. The simple attacks compress the files and upload them through FTP or through a HTTP POST request to a remote drop server. More sophisticated attackers obfuscate the data by XOR-ing it, encrypting it with proper asymmetric encryption or embedding it into media files using steganography to hide the data from traffic inspection. In addition to this, the amount of data sent and the timing can be chosen in a smart way. For example, some malware samples will send the data in smaller bursts so as not to swamp the network or generate network spikes that might attract attention. Since most employees use laptops, the malware can use location awareness to detect if the compromised computer is outside of the corporate network and send the data once it's directly connected to the Internet, such as from a Wi-Fi hotspot at an airport. This might allow the traffic to bypass perimeter security and receive less scrutiny. In some instances the infected computer might not have a direct connection to the Internet. In such cases, a previously compromised computer in the DMZ can act as a proxy, forwarding all the collected data.

Disruption phase

This is when any destructive payload is launched. If the attackers are only after information this phase might not happen at all. The targets and the goals for disruption attacks can be very different, there is no such thing as one-size-fits-all for disruption attacks. For example, Stuxnet was tailored to attack a specific uranium enrichment facility and would not work against a different target.

In recent times, wiper Trojans have been popular in attacks against the energy sector. The malware deletes all files

on a computer and then deletes the master boot record, rendering the computer unusable. This can happen on any operating systems and we have seen scripts for different UNIX flavors being used as well. Depending on the disaster recovery plan in place, these computers can be remotely recovered. However, there may still be an outage while the computers are being restored.

Resources

- [1] Marco Cova, Corrado Leita, Olivier Thonnard, Angelos D. Keromytis, and Marc Dacier. **An analysis of rogue AV campaigns. In Proc. of the 13th International Conference on Recent Advances in Intrusion Detection (RAID)**, 2010.
- [2] O.Thonnard, M.Dacier. **A Strategic Analysis of Spam Botnets Operations**. CEAS'11, Perth, WA, Australia, Sep 2011.
- [3] Jelena Isacenkova, Olivier Thonnard, Andrei Costin, Davide Balzarotti, Aurelien Francillon. **Inside the SCAM Jungle: A Closer Look at 419 Scam Email Operations**. International Workshop on Cyber Crime (IWCC 2013), IEEE S&P Workshops, 2013.
- [4] Olivier Thonnard, Leyla Bilge, Gavin O’Gorman, Seán Kiernan, Martin Lee. **Industrial Espionage and Targeted Attacks: Understanding the Characteristics of an Escalating Threat**. In Proc. Of the 15th International conference on Research in Attacks, Intrusions, and Defenses (RAID), 2012.
- [5] [Symantec Internet Security Threat Report](#) (ISTR), Volume 17, April 2012.



Author

Candid Wueest

Principal Software Engineer

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment—from the smallest mobile device to the enterprise data center to cloud-based systems.

Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

 Follow us on Twitter
[@threatintel](https://twitter.com/threatintel)

 Visit our Blog
<http://www.symantec.com/connect/symantec-blogs/sr>

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527-8000
1 (800) 721-3934
www.symantec.com

Copyright © 2014 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY . The technical information is being delivered to you as is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.