Winning the digital security battle: Cyber threat analysis from the Avecto Malware Labs
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>2</td>
</tr>
<tr>
<td>Threat landscape</td>
<td>2</td>
</tr>
<tr>
<td>Exploit kits</td>
<td>3</td>
</tr>
<tr>
<td>Malvertising</td>
<td>4</td>
</tr>
<tr>
<td>Sandworm</td>
<td>5</td>
</tr>
<tr>
<td>Ransomware</td>
<td>6</td>
</tr>
<tr>
<td>Java and Flash</td>
<td>7</td>
</tr>
<tr>
<td>Macro attacks</td>
<td>8</td>
</tr>
<tr>
<td>Threat landscape summary</td>
<td>10</td>
</tr>
<tr>
<td>Countermeasures</td>
<td>10</td>
</tr>
<tr>
<td>Case study 1 – CryptoFortress (Ransomware)</td>
<td>11</td>
</tr>
<tr>
<td>Case Study 2 – Macro attack (Key logger)</td>
<td>18</td>
</tr>
<tr>
<td>A Proactive Solution</td>
<td>24</td>
</tr>
<tr>
<td>Creating defense in depth with Defendpoint</td>
<td>24</td>
</tr>
<tr>
<td>Summary</td>
<td>27</td>
</tr>
<tr>
<td>Analysis Methodology</td>
<td>28</td>
</tr>
<tr>
<td>About Avecto</td>
<td>29</td>
</tr>
<tr>
<td>References</td>
<td>30</td>
</tr>
</tbody>
</table>
Introduction

In the rapidly evolving world of cyber security, attackers are continuously evolving their methods, launching new waves of malware to exploit weaknesses and infect systems. This creates challenges for both vendors and enterprise security teams, who are forced to respond with regular patches and updates. Following several high profile attacks and data breaches in 2014, the spotlight is firmly on security teams to protect their endpoints from increasingly advanced attacks.

With this pressure, security teams face a constant battle and a seemingly impossible compromise to balance risk without restricting user productivity. The key to success is to balance security and user freedom, with a strong security foundation that offers the flexibility needed for a positive end user experience.

This report from the Avecto Malware Labs will analyse some of the key trends within the security landscape, providing recommendations for dealing with some of the biggest threats.

It is difficult to evaluate the security of any system empirically as this would require consideration of all possible attack vectors. No product can claim to provide 100% protection against threats as this would require predicting the future. A more pragmatic approach is to examine the threat landscape to provide a measure of effectiveness. By reviewing the malware trends of the past 12 months, we are able to examine Defendpoint’s layered defenses and how this technology can reduce the risk of such attacks. We will then share technical case studies of common threats, to identify the most effective mitigation strategies.

Threat origins
The Avecto Malware Lab collects malware threats and intelligence from a wide variety of sources. We work with a number of organizations to capture and understand the behaviour of malware with the aim to test and develop our own technologies, as well as raise awareness of current threats. This approach provides valuable insight into how Defendpoint will perform in the real world and not just in a theoretical test environment.

“There are 387 new threats discovered every minute, equal to more than 6 per second.”
Threat landscape

As cyber security is an ever changing landscape, organizations need to be aware of the key trends in order to factor this intelligence into their defense strategies.

In reality, it is often the essential software at the core of the business such as web browsers and document viewers that introduce the most vulnerabilities to the endpoint. Organizations report that the browser is the primary attack vector 81% of the time (2) and for good reason. Internet Explorer alone had 240 vulnerabilities disclosed and patched in 2014.

The report will look at the most common types of threat and share insight into their behaviours in order to inform counter measures.

Exploit kits

Exploit kits have continued to dominate the threat landscape in 2014. These kits essentially provide an off-the-shelf package that can create, distribute and manage malware attacks utilising a variety of vulnerabilities. Sold by criminals on underground forums, they commonly target the web browser and plugins such as Java and Flash in an attempt to install malware on the target endpoint.

![Exploit Kits Prevalence in 2014](image)

Source: McAfee Labs, 2015.
Angler has become the most prevalent exploit kit due to its ability to avoid detection and bypass security products. It is used to distribute a variety of malware payloads such as Ransomware, banking Trojans and rootkits. It is often the first exploit kit to target new vulnerabilities. For example, last year it was the first to target Microsoft Silverlight.

A continual growth in exploit kits is expected as competition and demand grows. Previous attempts by law enforcement to take down exploit kits and their creators, as with the Blackhole kit, have only resulted in new products coming to market. Attempts to disrupt these kits only fuels further advances in their design, as prices and demand increases. This rapid evolution leaves traditional defenses struggling to keep up and organizations vulnerable to attack.

**Malvertising**

Malvertising campaigns, where adverts on trusted websites are replaced or infected with redirects to exploit kit attacks, are growing in number. Malvertising allows attackers to exploit the trust users have in popular and well known websites, as well as the large numbers of page visits they receive. A number of high profile websites receiving millions of visitors per day have been comprised in the past year, including Yahoo, The Huffington Post and Java.com. (3).

Despite attempts to tighten security, advertising networks remain vulnerable to content being manipulated due to widespread reselling and 3rd party hosting. This is a complex landscape, with many parties often involved in delivering the ad impression to the end user; from the agencies and media buying platforms to the ad networks themselves and the sharing sites that amplify the message.

The latest malvertising attacks have been combined with advances in real time ad bidding that allows advertisers to target specific industries or demographics by placing bids into an automated system. The result is highly targeted malicious adverts that are placed in the target user’s browser when they visit a trusted website. As these attacks only occur for a few hours and are precisely targeted, they are rarely detected – and this leads to long term infections.
A recent Malvertising campaign (5) saw over 1,700 real-time bidding ads that attempted to download a malicious SWF file onto the endpoint. This SWF file contains the CVE-2014-0569 (6) exploit which uses an integer overflow vulnerability to gain remote code execution. This allowed the attackers to install Ransomware such as Cryptowall when a vulnerable user browsed to the infected website.

Fast and targeted campaigns like these are often hard to spot and defend against. Keeping endpoints patched can help reduce some of the threats, but will not prevent against zero day attacks or the user being manipulated. All sites containing adverts should therefore be considered an increased risk, and as such, extra measures need to be taken to keep unknown threats isolated from the user’s data.

Sandworm
The past year has provided a number of interesting vulnerabilities including CVE-2014-4114 better known as Sandworm. This vulnerability affected all supported versions of Windows and allowed attackers to execute code on the target endpoint when they opened a poisoned office document. This was identified in the wild being used by a cyber-espionage group to target NATO members.

The vulnerability exploited a weakness in Microsoft Office that allowed documents to download and execute code from remote shares. This resulted in users being compromised just from opening an infected document. After the public disclosure, cyber criminals were quick to weaponize the vulnerability and package in exploit kits. These were used to target a series of Swiss banks with malicious PowerPoint documents that installed a variant of the Dyre banking Trojan (7).

This kind of zero day attack illustrates how dangerous it can be to rely on a reactive defense strategy. Although updates and patch management are important, organizations without proactive controls will remain vulnerable to unknown threats.
Ransomware
Ransomware has exploded onto the radar of security teams in recent years largely due to its aggressive tactics which are difficult if not practically impossible to recover from. It’s big business too - Cryptolocker affected over 0.5m systems in a 9 month period during 2014, reportedly earning its creators $3m.

The premise is simple; capture data that is valuable to the user by encrypting it in situ and then demand a fee to release the data back to them. Payment servers are hosted on the Darknet and anonymous crypto currencies such as Bitcoin are used to make the ransom payments and the criminals are almost impossible to trace. Ransomware has changed the landscape because response teams that were used to dealing with stealthy malware and hidden banking trojans are suddenly confronted with bold malware that grabs data and informs their users directly. The risks of wide spread data loss are huge and growing ever larger as ransomware begins to target network shares as well as the user account.

The real power of these attacks is the way in which they exploit the access and tools available within Windows. When a user unwittingly runs Cryptolocker, it has access to all of the user’s files. This means that even in cases where the user does not have admin rights, a large amount of data is vulnerable. Ironically, in these cases, the cryptographic tools that usually secure data in Windows are exploited to encrypt files. The result is a devastating attack that requires little code or technical skill to create.

Reactive technologies such as antivirus simply cannot keep up with the rapid development of ransomware. Due to the fast and aggressive nature of the threat, the majority of detection and network based tools may only alert you to the danger when it is too late and the damage has been done. As it only takes one standard user account to inflict significant damage, defenses should be built from the endpoint out.
Java and Flash
Java and Flash vulnerabilities have continued as a major threat vector due to the prevalence of organizations running outdated and insecure versions. Research conducted by Avecto in 2015 revealed that 55% of councils in England are at risk due to unsupported, vulnerable versions of Java. Councils are not alone in falling behind though, as organizations around the world struggle to keep up with a constant stream of patches from these vendors.

The risk is significant because many businesses are forced to run vulnerable versions of Java to maintain compatibility with core business applications. This is evident when we investigate the exploits commonly used by an attacker. Java vulnerabilities patched in 2012 are still being used by Magnitude and Rig exploit kits proving that many are failing to patch and upgrade (8).

Organizations are increasingly looking for ways to contain these threats with technologies such as sandboxing. If these attack vectors can be isolated and contained, the risk of enabling them is mitigated.

Macro attacks
Once thought to be a distant memory of the 1990’s, macro attacks in Office documents have started to reappear. Microsoft originally fixed the problem of malicious macros by preventing them from running without the user’s permission. These latest attacks actually draw upon users being aware of secure technologies such as encryption to circumvent this by manipulating the user into enabling macros and allowing the attack to run.

The victim opens a seemingly important document that appears scrambled apart from the heading which informs them the document is securely encrypted and they need to enable macros to view the document safely. If macros are enabled the victim sees the contents of the document “decrypt” and become legible, while in the background a malware payload is running, resulting in users not even realizing they have been compromised.
Microsoft has charted a significant increase in macro attack campaigns against US and UK customers in 2014. These attacks are often linked to fake legal or financial threats, in order to pressurize the user into opening the fake invoice or legal document and enabling the macros. The technical implementations of these attacks vary wildly, however the majority of the attacks prefer to use older Word 1997-2003 documents. They often attempt to harness the user’s access to native Windows tools such as Command Prompts to download and execute payloads.
Although user education can go a long way to limiting the effectiveness of these attacks, it will never provide full protection and cannot be relied on entirely. Some recent attacks have been very sophisticated researching and directly targeting high value users with convincing documents containing encrypted payloads.
Threat landscape summary
Avecto’s Malware Lab has reported larger volumes of attacks than ever, with malware threats evolving at great pace. As security has increased, the attackers are increasingly looking to manipulate the trust of end users, either by tricking them into opening a file or by exploiting the access and tools available in Windows. As users need to open documents and view websites in order to perform their job roles in today’s digital society, it is becoming harder to draw the line in terms of security and control.

The traditional security model has been to try and define the known bad, and then catch and block it using a blacklisting model. However, in the current landscape, organizations should strive to create layered defenses that define key areas of known good applications, while isolating the unknown so that threats are contained.

Countermeasures
This paper will go on to examine the behavior of specific malware and suggest recommended countermeasures based on a proactive security approach. With traditional detection based technologies struggling to keep pace with the rapid rate of change.

A layered approach utilizing proactive technologies to create defense in depth is the most effective form of securing the endpoint against advanced attacks. This paper will now go on to explore this in more detail, explaining how Avecto’s Defendpoint software combines Privilege Management, Application Control and Sandboxing to form an integrated suite that protects against the latest malware attacks.
Case study – CryptoFortress

CryptoFortress ransomware follows in the footsteps of the notorious Cryptolocker malware and represents the latest generation of ransomware. This strain of malware encrypts photos, videos and documents on local, network and USB drives for maximum impact. CryptoFortress is a stripped down version of the last generation of ransomware (TorrentLocker), implementing a basic but effective feature set. The result is a small executable, less than 100kb in size, containing less tell code that could be detected by antivirus engines.

<table>
<thead>
<tr>
<th>Delivery mechanism</th>
<th>Exploit Kit (Nuclear)</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Encryption</td>
<td>AES-256 ECB</td>
</tr>
<tr>
<td>Key Encryption</td>
<td>RSA-1024</td>
</tr>
<tr>
<td>Crypto Library</td>
<td>Microsoft Crypto API</td>
</tr>
<tr>
<td>Payment Page</td>
<td>Tor anonymous network</td>
</tr>
<tr>
<td>Payment method</td>
<td>Bitcoin</td>
</tr>
</tbody>
</table>
This malware has been spotted in the wild being distributed in malvertising campaigns. The malicious adverts redirect the user through several recently registered domains to a Nuclear exploit kit landing page, hosted by a VPS provider in the Netherlands. The IP ranges detected in the attack appear to have been serving a number of suspicious payloads recently:

<table>
<thead>
<tr>
<th>Date</th>
<th>Payload requested</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-03-06</td>
<td>131.72.138.***/install.exe</td>
</tr>
<tr>
<td>2015-03-03</td>
<td>131.72.138.***/Pony2.exe</td>
</tr>
<tr>
<td>2015-03-03</td>
<td>131.72.138.***/download.exe</td>
</tr>
<tr>
<td>2015-03-03</td>
<td>131.72.138.***/adobe_flash.exe</td>
</tr>
</tbody>
</table>

Payloads delivered by exploit kit

This attack chain follows the classic pattern of malvertising by injecting a malicious advert into a legitimate page, and then uses this to redirect the user. The user is bounced around redirect sites before arriving at the exploit kit landing page. The landing page attempts to identify if the user is running any vulnerable software, and if successful, delivers a targeted exploit.

Malvertising attack chain

The malware threat was not detected by any of the 57 anti-virus products tested.
Technical deep dive

The sample captured in the Avecto Malware Lab appeared to be impersonating a legitimate Adobe update “adobe_flash.exe”. Initial analysis revealed that the file was not detected by any of the antivirus engines and even after 10 days there were still 19 that had not detected the malware. As this particular sample only existed in the wild for a few days, it is reasonable to assume that the attackers regularly re-engineer the malware to avoid detection. Some research has even suggested that cyber-criminals use services such as VirusTotal.com to test the evasion capabilities of their malware against the most popular antivirus software (9).

Initial testing of the CryptoFortress payload was unsuccessful with the process terminating almost immediately. Further investigation revealed that the malware implemented a number of tactics to evade detection and reverse engineering. The malware queries a number of system properties and tests for the presence of a debugger. If any emulation or reverse engineering attempts are detected the process terminates. Once we reconfigured our lab environment to bypass these checks, the malware decrypted and ran the ransomware payload.

Consequence

Unlike previous generations of ransomware, the malware wastes no time contacting command to control servers, starting the encryption process almost immediately. CryptoFortress is very efficient targeting network shares as well as local and mapped drives simultaneously, encrypting all documents, videos and images. Once encrypted files remain on disk with an “.frtrss” extension appended to the filename.

Encrypted files and a ransom demand
The malware also attempts to silently delete all shadow copies of the file system to prevent the user recovering data. This is achieved using the following command:

```
vssadmin delete shadows /all /quiet
```

Early versions of ransomware stored the encryption key on disk leading to advanced users being able to decrypt their files for free. The latest threats have evolved though, and once the encryption is complete the malware releases the encryption key and exits, leaving no realistic way to recover the decryption key without making payment.

Once the encryption has completed, users are presented with a HTML page almost identical to that used by TorrentLocker. However, it is unclear if this malware is published by the same author or if they are just reusing code. The HTML files, named “READ IF YOU WANT YOUR FILES BACK.html” are also placed in every folder containing encrypted files to alert users of shared drives, as well as the logged on user.

Payment page
The ransom demand is set to one Bitcoin which at the time of publication, is currently demanding around $300, and multiple sources to buy are suggested to the user. The server used for payment and decryption is hosted on the Darkweb hidden within the anonymous Tor (the Onion Router) network. The Tor network encrypts and relays internet traffic anonymously through random nodes to hide the origin. This provides a high level of protection for the attackers, with both the payment method and control server almost impossible to trace.

Interestingly, the malware offers to decrypt two files smaller than 500kb as a show of good faith before paying the ransom. However, victims of this attack should be urged not to test this with sensitive data as even though it avoids payment, this action still sends the file to the attacker’s server.

Countermeasures
Traditional security technologies are failing to keep up with the latest malware threats as they are based on a reactive model. Encryption of data now begins in seconds, whereas antivirus detection can often take days, leaving the user at risk. In order to limit exposure to these type of threats it is important to keep vulnerable web applications updated with a robust patching strategy as part of a layered security approach, to limit the attack vectors against the endpoint.

The level of user access can also play a significant role in limiting the ransomwares access to data. If the compromised user is an administrator, the ransomware can exploit the wide access of the user to encrypt more data and gain deeper access to the system. If the user has a standard user account, the threat could be contained to their data and network access, restricting the impact of an attack.
The issue is that even a standard user will have access to large amounts of valuable data on the endpoint and network shared drives. This demonstrates the importance of utilising multiple complementary technologies to achieve holistic security. For example, endpoint sandboxing technologies extend your protection by isolating threats away from the user’s data using a secure container to segregate the malware. In the event that ransomware does execute, it will have no access to the user’s data from within the sandbox environment.

Whitelisting is often cited as the number one defense strategy against real world attacks, and for good reason. Had this system been whitelisted, the dropped CryptoFortress executable would have been prevented from executing. Many organizations have traditionally dismissed whitelisting solutions as they are often perceived to be too complex and time consuming to manage and scale. However, next generation technologies that take a more pragmatic approach combining whitelisting and removal of admin rights to provide trusted areas of the build finally make this strategy straightforward and achievable.

Robust backup procedures can help the recovery process following such incidents, however these should be an absolute last resort as prevention is always better than the cure. To that end, it is always better to be able to block an attack than recover from an attack. If the attacker can encrypt files they can also exfiltrate data leading to a data breach. With high profits to be made and little chance of being caught, organizations should expect ransomware attacks to continue to create security challenges in 2015 and beyond.
How Defendpoint stands up to ransomware

Defendpoint is designed to protect the user’s data as well as the endpoint, by offering layers of proactive defense that build to form simple yet holistic defense in depth. The Sandboxing module allows users to securely browse the web and view documents without risking exposure of sensitive data. It works by ensuring that potentially vulnerable internet-facing content is seamlessly opened in a secure Sandbox environment, isolating and containing the threat.

In the event that a browser or plugin is exploited, the attack is effectively isolated in the context of another user account, which blocks threats from ever accessing the user’s actual profile and data. Defendpoint’s Application Control capabilities can also block the executable payload from ever running so that the ransomware is unable to access and therefore cannot encrypt any of the user’s files. This unique approach ensures Defendpoint is able to proactively stop attacks, without relying on signatures or detection methods.
Case Study – Macro attack

Cyber criminals are highly opportunistic and will often take events in the news and try to capitalize on them with themed malware campaigns. As US tax returns season began, we witnessed such a campaign in our labs starting with spoofed tax phishing emails.

The purpose of the email is to get the user to open a document believing it contains details of a complaint and potential IRS investigation. This type of attack is very common and highlights the dangers of unsolicited emails.

Macro attack chain

User downloads malicious document  ➔  Document claims to be encrypted  ➔  User enables macros to “decrypt”

User downloads malicious document  ➔  Document claims to be encrypted  ➔  User enables macros to “decrypt”

Dropper service begins downloading and executing further malware  ➔  Document shows plain text, user closes  ➔  Macro script downloads malware dropper to Temp folder

Technical deep dive

The email spoofed a seeming legitimate IRS email address and provides the correct contact details in the body of the email. The user is urged to review the document before contacting the IRS.

Spoofed email address

Tue 27/01/2015 14:55
Internal Revenue Service <complaints@irs.gov>
Complaint against your company
Legitimate IRS contact details are provided

Analyzing the email header, we see that it originated from 81.130.214.*** a UK IP address allocated to a home broadband provider, likely to be a user previously compromised by an attacker. The return email address was set to that of a property holding company in the Caribbean, again likely compromised by the attacker.

The phishing email contained a link to a document “legsal_complaint20150127.doc” hosted on a 3rd party cloud storage provider. Our lab found that only 4 out of 56 AV engines flagged the file as potentially malicious. After 10 weeks, only 12 out of 56 flagged the document as a threat.
The downloaded document contains a malicious macro and once extracted we can quickly see how it is bypassing the signature-based detection of AV engines. The code uses some fairly simple obfuscation techniques to bypass detection, breaking apart strings and combining with individual characters. This technique is commonly used in a variety of exploits.

```
FILENDIR = “c:\” + Chr(Asc(“U”)) +“sers\”+ USER
+“\AppData\Local\Temp\”
```

Example of obfuscation

The purpose of the macro script is to execute a batch script via cmd.exe which checks connectivity then executes a PowerShell script. Utilizing Windows tools such as PowerShell has become a common malware tactic. It allows the malware code to be smaller and also appear less suspicious by using Microsoft products. The PowerShell script downloads and executes a payload named “install.exe” located on the attacker’s server.

**The payload then performs several steps:**

- Collects system information (MachineGuid, SystemBiosDate)
- Copies itself as “winlogin.exe” in the system temp and app data folders
- Sets fake “winlogin.exe” to run at start up
- Connects to various websites to test connectivity

Once the malware has successfully installed itself onto the victim’s system, it begins logging the user’s keystrokes. This can be seen by searching for strings in the malware processes memory where we see the keystrokes being recorded in plaintext.
Plaintext of key logger captured in memory

These captured logs are then regularly posted to the attacker’s command and control server, using HTTP POST to a '/log/index.php' page. The malware uses a domain generation algorithm to rotate the web address it transmits data out to every 24 hours, this reduces the chances of network controls detecting and blocking the communications.

Consequence
The consequences of a key logger running on a system could be disastrous. The attackers could capture a wide variety of login details, as well as sensitive corporate and personal data. This type of attack is often used in early stage reconnaissance of a target or as an opportunistic way to harvest login credentials.

The attack uses process names such as winlogin.exe and regularly changes the domain name it reports back to in order to remain undetected for as long as possible. From the attacker’s perspective, the longer they can operate, the more valuable information they can capture.
Countermeasures
As the threat remains largely undetected by traditional defenses even after several weeks, a different approach is needed. As always, user privileges play a large role in containing the threat. It is far better that the malware is not given easy access to admin rights in order to limit the potential damage. Without admin rights, the malware cannot embed itself deep within the system or spread to other local user accounts. This however still leaves the initial user compromised.

Securing systems using two factor authentication can prevent stolen usernames and passwords being exploited by the attackers. Whilst we would always recommend that two factor authentication is used this is a last resort as it does nothing to prevent the theft in the first instance.

A more proactive approach would be to implement whitelisting and use Application Control to prevent the payload from executing. The early stage of this attack utilized Windows tools such as PowerShell and the Commandline to download and execute malware on the disk. Using Application Control we could block access to these tools, however this traditionally would prevent the user from accessing them as well.

Using a layered approach with Sandbox isolation, we can add an additional secure whitelist just for vulnerable internet facing content within the Sandbox, providing much tighter control and security.

Isolation of untrusted content in a Sandbox environment provides the perfect context for enhanced Application Control rules. For example, we can block untrusted content in the Sandbox from accessing PowerShell without preventing the native user from using it. This provides a powerful mechanism for defending the user without limiting their environment.
How Defendpoint stands up to macro attacks
Defendpoint is designed to offer a proactive layered approach to security.

In this macro document attack, the Defendpoint user was protected from the very moment they clicked the malicious link. Defendpoint’s Sandboxing module opens the browser viewing the link in a secure Sandbox, containing and isolating the threat.

When the document is saved to disk, Defendpoint tags the file as untrusted so that it is never allowed access to the user’s profile and data. The document automatically opens within the Sandbox whenever it is opened. Even if the user enables the macros, Defendpoint’s Application Control technology prevents the untrusted content from using the command line to download and execute payloads. This ensures that user is able to open and view an untrusted document without risking the endpoint being compromised.
A proactive solution

When testing malware in our labs, we found that a proactive and layered approach can prevent the vast majority of real world threats. This is supported by research from the Council on Cyber Security with SANS and the Australian Department of Defense, who found that technologies such as Application Control and Privilege Management were far more effective defenses against real world attacks than antivirus – listing them both in their top 5 security strategies.

When testing in our labs, samples are run against virustotal.com to get an indication of antivirus detection rates. The majority of threats had little or no detections for the first 24 hours, and after 48 hours we generally saw a sudden detection increase to an average of 15 vendors with the rest catching up over the next 10 days. This is supported by the Ponemon (2) findings that 81% of web-borne malware can be completely undetectable.

Technologies such as IOC, Network based detection and Firewalls do provide some benefit, however they ultimately suffer from the same flaws. They are trying to detect known bad behaviour or events generated after the damage has been done. Whilst these have a place in the defense stack, proactively protecting the endpoint should be the main focus, as ultimately this is where threats will land if they are not detected.

This delay in detection times demonstrates the need to move beyond the traditional security model and layer up proactive defenses that are not reliant on signature or blacklist based concepts. Instead, we recommend moving towards models of trust and controlled access.
Creating defense in depth with Defendpoint

Defendpoint protects your endpoints against advance threats, protecting the system, user and safeguarding private data. Defendpoint’s single client provides three powerful technologies that layer together to form the core of a proactive defense in depth strategy. Through the removal of admin rights with Privilege Management, plus Application Control and Sandboxing, Defendpoint mitigates the risks of malware and cyber attacks.

Let’s look at how Defendpoint protects endpoints from the known threats of today as well as the threats of tomorrow.

**Privilege Management** – Removes admin rights from the user and only assigns them directly to known trusted applications. This prevents malware from exploiting the user’s rights to disable security features and spread.

**Application Control** – Contextually aware whitelisting allows you to take control of untrusted internet content. Payloads are blocked from executing and access to system tools such as PowerShell is prevented. Trusted native content is unaffected and key areas of the build can be whitelisted to make application control simple.

**Sandboxing** – Allows you to securely and seamlessly isolate websites and documents from the internet. This prevents malware from being able to access, encrypt or steal private data. Files originating from untrusted sources are automatically contained allowing the user to view, edit and save them without risking all their data. This unique approach to Sandboxing harnesses core Windows security technology to provide a powerful but lightweight Sandbox.

This unique combination has proven to be highly successful in defeating malware threats that are currently plaguing organizations. Threats such as Exploit Kits, Ransomware and Malicious documents are contained or blocked by Defendpoint’s revolutionary approach to endpoint security.

Our case studies have shown how without Defendpoint in place, malware can bypass detection and cause serious damage. However, with Defendpoint deployed, these threats are prevented from ever running on the endpoint.
How Defendpoint thwarts the attacks

In practise – how Defendpoint protects your users
The below summary table illustrates how the two attacks described in this report would have been mitigated with Defendpoint.

<table>
<thead>
<tr>
<th>Case Study</th>
<th>Without Defendpoint</th>
<th>With Defendpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ransomware</td>
<td>Malware executes as the user - Data encrypted</td>
<td>Malware payload caught in the Sandbox and blocked by Sandbox aware Application Control - Data protected and malware wiped on reboot</td>
</tr>
<tr>
<td>Macro attack</td>
<td>Malware executes as the user – Key Logger is installed</td>
<td>Document isolated in the Sandbox and Application Control prevents cmd.exe being used to download payload – Payload is never downloaded or executed</td>
</tr>
</tbody>
</table>
Summary

IT security breaches are now at the highest level in UK history, with 200 new threats per minute being discovered by McAfee, while traditional antivirus measures are effective less than half of the time. This constantly changing and evolving malware landscape continues to create challenges for the enterprise, with the focus of many malware writers now turning towards the user in order to exploit trust and gain entry to corporate data.

Our lab test and third party evidence suggests that the most effective form of defense is taking a proactive standpoint with security layers that prioritize key measures. Ensuring you have perimeter defenses is important but the traditional “egg shell” approach to security where the outer layers are tough but the inside is soft, is no longer enough.

A multi-layered approach combining antivirus, firewalls, patching, Application Control and Privilege Management provides a solid security core, with Sandboxing adding a vital last line of defense. With 58% of security professionals expecting even greater pressure to secure their organization against threats in 2015 (11), now is the time to get proactive.

It’s time to stand up to advanced attacks.

To learn more, visit avecto.com

“Let us not look back in anger or forward in fear, but around in awareness.”

James Thurber
Analysis Methodology

In our labs we built a secure test environment with a clean version of Windows 7. As some of the malware samples contained advanced anti-sandbox features the virtual environment was configured to prevent detection by anti-sandbox techniques.

Common anti-sandbox checks included checking for the presence of:

- vmusbmouse.sys or vmmouse.sys (VMware)
- vboxmouse.sys or vboxvideo.sys (Virtual Box)
- prl_mouf.sys or prl_sound.sys (Parallels)
- Checking for virtual keyboards
- Delayed decryption of payload
- Checking for non-existent websites (test environments may generate response)

All of the malware samples tested were live samples captured from websites and email campaigns. In cases where the Exploit Kit targeted specific versions of the browser or plugins the appropriate version was installed.

Each sample was executed multiple times and given several hours to run in order to detect any delayed payloads, a common technique used to fool network defenses or AV scanners. After each sample was analysed the virtual machine was restored to an original clean state to prevent cross contamination.
About Avecto

Avecto is an innovative technology business specializing in endpoint security software. The company’s revolutionary Defendpoint software ensures security defense in depth while empowering users to work freely. This mantra of security + freedom underpins Avecto’s philosophy to unite IT departments and their end users.

Established in 2008, Avecto is headquartered in Manchester (UK) with offices in Boston (USA) and Melbourne (Australia), supported by a network of worldwide channel partners.

Avecto’s experience is proven, with implementations of over 5 million endpoints at many of the world’s most recognizable brands, from the largest banks and most highly regulated government organizations to multichannel retailers and F1 teams.

Attention to detail is paramount, with a team of qualified and experienced technology consultants on hand to guide clients through a robust implementation methodology. This consultative approach provides clients with a clearly mapped journey against measurable objectives to ensure project success.

Avecto has placed in the top 4 of the Deloitte Fast 50 for the last two consecutive years, making it one of the UK’s fastest growing software companies, winning global accolades for quality and innovation.
References


