SOPHOS
Security made simple.

Defeating the Targeted Threat - Bolstering Defenses with a Sandbox Solution

In the continuing arms race between cyber criminals and the organizations whose data they covet, we continue to see new, ever more sophisticated, tools being deployed on both sides.

Lately, attacks called advanced persistent threats (APT) which were originally used only against very large organizations have become more common and are now being used against smaller companies, either to attack the smaller entity itself or as a stepping stone to other larger targets. This was evident in the attacks on Target Stores and Home Depot, two large US retailers. Both companies were breached using stolen credentials that had been given to a smaller supplier.

This has thrown the spotlight on small and midsized businesses.

Small and midsized business are on the radar of attackers, who actually see them as low hanging fruits because many of them lack the resources, the security and the multi-layer defense programs to help protect themselves. 42% of small businesses[2] report being a victim of cyber-attacks and the majority of the companies hacked were hacked twice or more.

On average, small businesses report $32,000 being stolen from bank accounts with the majority of them taking a week or more to resolve the issue.

£34 billion is the annual cost of data breaches for UK Businesses[1]

Growing Awareness

On a positive note, we are seeing a rise in security awareness driven by the increased coverage of cyber threats in the mainstream media. This has helped many organizations improve their security posture: Employees see news about cyber-attacks and develop more awareness of security risks and so are less likely to engage in risky online behaviour; senior management understand the risks more clearly so IT departments find it easier to obtain the budget required to strengthen and improve their defences.

Demand for Comprehensive Next-Generation Security Solutions

IT teams in organizations of all sizes now understand that sophisticated cyber-attacks can use unknown malware that can evade traditional gateway and endpoint protection. This is why many organizations are considering new solutions to combat this problem. Additionally, there's a lot of hype encouraging you to buy additional next generation solutions to deal with these unknown threats.

However, often these technologies are too complex and expensive for many businesses to consider. Many of the complex security solutions used by larger enterprises require multiple dedicated devices which are resource and maintenance intensive. They also tend to have low accuracy; this means a skilled team is required to analyse the results. Buying more solutions from multiple vendors that don't talk to one another isn't a recipe for a manageable threat defense.

Emergence of Advanced Threats that Fly Under the Radar

Advanced Persistent Threat (APT)

An APT is a network attack in which cyber criminals use custom-developed targeted attacks to gain access to a network and remain undetected for long periods of time. While simple attacks use the smash and grab technique (get in and out quickly to avoid detection), the success of APTs depends on staying under the radar as long as possible. For this to happen, they use evasive coding techniques and a series of advanced manoeuvres to slip past traditional security barriers and steal sensitive data.

74% organizations think they will be hit by an APT in the near future[3]

Advanced Evasion Technique (AET)

This is a cyber-attack that uses numerous known evasion tactics to create a single new tactic, whose intrusion cannot be detected by traditional security products. While the AET might not be malicious, its core purpose is to provide the attacker with access to an organization's network that remains undetected.

New Age Threats Need Next Level Security – Sandbox

One technology, that's had more than its fair share of hype, is the sandbox.

The questions you are probably asking yourself around sandbox technology are:

1. What is a sandbox?

2. Do I really need a sandbox?

3. Why don't my conventional defences protect me from these APTs?

4. Surely this kind of technology is for larger organizations?

5. Another point solution? That sounds expensive.

6. It sounds complicated – do I have the resources to try and deploy this?

7. How do I choose the right sandbox?

Let's answer each of these questions one by one:

1. What is a sandbox?

A sandbox is an isolated, safe environment, which imitates an entire computer system. In the sandbox, suspicious programs can be executed to monitor their behavior and understand their intended purpose, without endangering an organization's network.

2. Do I really need a sandbox?

Organizations need a range of security technologies to protect them from threats both known and unknown. It's likely you'll already have deployed Secure Email Gateway, Secure Web Gateway, UTM or Next Generation Firewall at your internet gateway, as well as endpoint protection to your desktops and servers.

Even vendors that only supply standalone sandbox technology would never suggest that their product provides a complete defense against advanced persistent threats. They acknowledge that many security layers are essential to protect against these threats. What a sandbox does provide, is your own dedicated environment to analyse, understand and take action, on the threats to your organisation that haven't been detected by this stack of conventional security measures. Sophisticated targeted malware, designed to evade detection, will be detected and blocked when detonated in your sandbox.

3. Why don't my conventional defences protect me from these APTs?

Basic signature-based antivirus will protect you against known malware. But signature-based antivirus is reactive and increasingly outpaced by today's attackers. Most leading security vendors use a range of approaches such as malicious traffic detection capabilities and emulation to supplement signature-based detection. However, if your data or credentials are valuable enough to the attacker, they will have spent time discovering what type of security you are using and tested their unique malware to ensure that it will evade detection by your defenses

4. Surely this kind of technology is only for larger organizations?

The attack on Target Stores resulted in 40 million credit card numbers stolen. This had an enormous impact on trust in the Target brand and led to the company spending a significant amount of money on breach-related expenses, like providing monitoring services to protect customers from fraud. Target is certainly a large organization, but what's important to consider is that the attackers stole the credentials of Target's air conditioning contractor. This small supplier was seen as a soft target and an easier route into the larger business. So organizations of all sizes should consider sandbox technology; a targeted attack could cost you your key customers and is one factor in the statistic that 60% of small firms go out of business[4] within six months of a data breach.

5. Another point solution? That sounds expensive.

Sandbox can be expensive, no doubt. But there are ways of reducing your costs. In their research note on network sandboxing Gartner recommends:

"If your organization is budget-constrained or looking for a quick path to add sandboxing, first evaluate adding sandboxing as a feature from one of your current security vendors."

Your existing UTM, Firewall, Secure Web Gateway or Email Gateway may have sandboxing-as-a-feature options available.

With the introduction of cloud computing, the way processing power and storage is delivered and priced has changed. Companies now have access to greater processing power at affordable prices. This has driven a revolution in what can and can't be delivered as a service. Services like AWS are changing how we think about process intensive solutions.

Sandboxes have proven very effective in identifying and stopping APTs by creating a full working environment for the malware to operate in and making it hard for it to identify that it is being analysed. Previously, such a complex solution had to run on dedicated hardware and have a team of analysts to decipher the results limiting it to large enterprises and malware research labs.

By moving sandboxing to the cloud, the reduction in cost means security vendors can apply more processing power and share resources across multiple customers. It also means companies no longer have to rely on in-house expertise as their vendors or partner can provide the analysts from a central location. This reduces the costs to such a level that all organizations can afford sandboxing.

6. It sounds complicated – do I have the resources to try and deploy this?

When you begin to trial solutions, consider solutions that are easy to try and deploy. Cloud-based solutions can be rapidly deployed giving you instant results without the need to deploy hardware or upgrade appliances.

7. How do I choose the right sandbox?

Choosing a sandboxing solution will be a challenge considering the numerous options available on the market. Consider the following points while making a choice:

- **Analyze a broad range of suspicious objects**

Pick a solution that can detect threats designed to evade sandboxes. Your sandbox needs to be able to analyse a broad range of suspicious files – check that your chosen solution can analyse archives, Microsoft Office documents and pdfs, as well as executables.

- **Comprehensive operating system and application stack coverage**

Comprehensive platform coverage is important so that malware that has been fine-tuned to run only in a specific environment can be detected.

- **Contextual information about the malware or targeted attack**

Context about the targeted attack is mission critical. You need a solution that can give you visible protection with granular incident based reports that provide this context.

- **Sandbox Analysis Rate**

Choose a solution that filters files using antimalware and reputation services to reduce the number of wrongly convicted files and the number of files sent for sandboxing. This helps ensure there is minimal impact on performance and that your users are not disrupted.

- **Collective Security Intelligence**

Choose a solution that uses the collective intelligence of all sandboxing events so you can benefit from all customer threat analysis. Conventional security checks fail to discover all breaches; therefore the need of the hour is to improve the accuracy of detecting unknown threats. For this to happen, it is imperative to adopt a hive-minded approach to IT security, which uses cloud-based collective threat intelligence from multiple events and customer implementations.

Introducing Sophos Sandstorm

Sophos Sandstorm is an advanced persistent threat (APT) and zero-day malware defense solution that complements Sophos security products. It quickly and accurately detects, blocks, and responds to evasive threats that other solutions miss, by using powerful, cloud-based, next-generation sandbox technology.

Highlights:

Advanced protection from targeted attacks

Sophos Sandstorm provides the advanced protection organizations need to combat unknown threats - and we make it simple and affordable to buy and maintain.

Simplicity

Sophos Sandstorm is fully integrated into your Sophos security solution. Simply update your subscription, apply the Sandstorm policy and you're protected instantly against targeted attacks.

You'll be up and running in minutes.

Block evasive threats that others don't see

Detect unknown threats specifically designed to evade first-generation sandbox appliances. Our full-system emulation approach provides the deepest level of visibility into the behavior of unknown malware and the detection of malicious attacks that others simply miss.

Deep forensic reporting

Accelerate response to advanced threats with simple incident-centric breach analysis. We provide you with prioritized APT intelligence by correlating the evidence. This approach both reduces noise and saves you time.

Comprehensive analysis

Determine potential threat behavior across all your end user devices and critical infrastructure. This includes your operating systems (Windows, Mac OS X, and Android); physical and virtual hosts; services; users; network infrastructure; and web, email, file, and mobile applications. Safely detonate threats in the Sandstorm cloud, isolating your datacenters from dangerous malware.

Lightning performance

Your Sophos security solution accurately pre-filters traffic, so only suspicious files are submitted to Sandstorm, ensuring minimal latency and end user impact

Conclusion

Your organization's security posture needs to evolve keeping in mind the advanced and targeted nature of new age threats. The sandbox not only bolsters your IT security infrastructure but also takes it to the next level. The need to protect your organization from unknown evasive threats is best served by a solution that addresses the limitations of traditional antimalware signatures. For many companies, advanced technologies are too expensive and require additional security expertise to implement and monitor them. Sophos is changing this by providing all businesses access to a next-generation sandbox solution that's affordable and simple to deploy.

If you'd like to find out if Sophos Sandstorm is the right solution for your business, get in touch - find out more at sophos.com/sandstorm.

1. Centre for Economics and Business Research (CEBR)
2. National small business association report 2015
3. ISACA Advanced Persistent Threat Awareness Study Results
4. Huffington Post

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA

SOPHOS