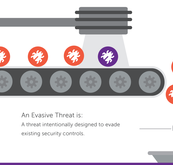
Outmaneuvering Advanced and Evasive Malware Threats

DELL SecureWorks

What are Advanced and Evasive Threats?

A cyber attack exploiting a vulnerability in software where the vulnerability is not known across the general security community. It's the threat CISOs fear the most because there are no countermeasures currently written for it.

Evasive Threats



An Evasive Threat is:
A threat intentionally designed to evade existing security controls.

Advanced Threats

An Advanced Threat is:
A targeted threat. It may be 'off-the-shelf' and been seen before, or be a zero-day threat.

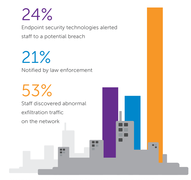
The Pain

"No matter how many times you save the world, it always manages to get back in jeopardy again. Sometimes I just want it to stay saved! You know, for a little bit? I feel like the maid; I just cleaned up this mess! Can we keep it clean for... for ten minutes!"
"Bob," otherwise known as Mr. Incredible

44% Forty-four percent of respondents reported a major increase in the number of malware incidents targeting their endpoints.

40% Forty percent said their endpoints had been the entry point for an Advanced Persistent Threat (APT)/ targeted attack in the last 12 months.

How victims learned of APT/targeted attacks across their organizations:



Ponemon Institute, "2014 State of Endpoint Risk," December 2013, survey of 647 IT and IT security professionals with involvement in endpoint security

Malware evasion

Detect the Sandbox Environment
Malware is crafted to look for indicators and objects that suggest a sandbox environment is present and delay operations that could reveal itself.

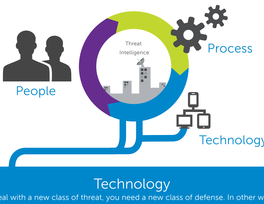
Avoids being analyzed
Malware may introduce timing delays to "sleep" for a defined period while a sandbox is likely monitoring to trick the system. Or, the malware waits until someone clicks something or a reboot happens on the system.

Application Targeting
Malware may efficiently target only key systems to avoid being flagged by the general security community. For example, malware targeted at point-of-sale systems is smart enough to move on if it encounters a non-POS system.

The Solution

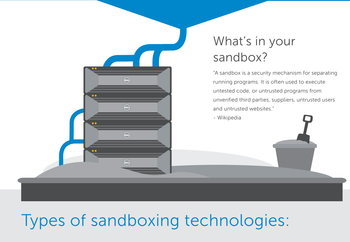
Recent security breaches create a new imperative for the optimal blend of people, process and technology fueled by intelligence for security to be effective against zero-day, advanced and evasive threats.

To achieve inner security peace:



Technology

To deal with a new class of threat, you need a new class of defense. In other words, you need "Advanced Malware Protection" or "AMP" which is an industry term for technology designed to continuously monitor for, offload and detonate files safely away from the main environment to observe and detect malicious objects.



What's in your sandbox?

"A sandbox is a security mechanism for separating running programs. It is often used to execute untested code, or untrusted programs from unverified third parties, suppliers, untrusted users and untrusted websites."
- Wikipedia

Types of sandboxing technologies:

OS Emulation

OS emulation provides a high level of malware behavior visibility by emulating at the operating system level. However, as a result, it's easier for malware to crack.

Virtual-Machine

VM sandboxing offloads malware to virtual machines that replicate the targeted environment. It provides a low level of visibility of malware behavior but up to now has been harder for malware to crack.

Full-system Emulation

Full-system emulation sandboxing simulates the target environment at the physical hardware level (CPU and memory) to convince the malware that it is running on the target system's hardware. As a result, it is the hardest approach for malware to crack.

Source: **Lastline, Inc**

The Right Expertise

If a security device produces an alert in the forest, who's there to hear it? The best technology means nothing if you don't have the right expertise to react to the alert, quickly decipher complex reports, investigate the threat, and determine the right response.

Required expertise

Deep technical and analysis acumen to research the threat and (connect the dots)

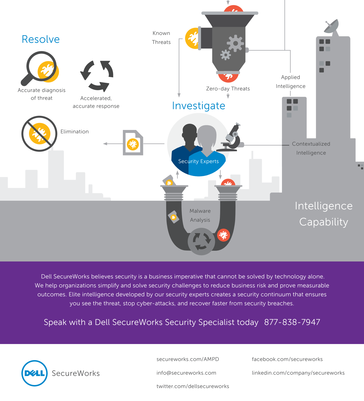
Malware analysis/reverse engineering

The Intelligence

Intelligence is having a vast library of information and insight on threats and threat actor tools, techniques and procedures – otherwise known as pre-knowledge. A zero-day threat is not a zero-day threat if it's been seen before.

The Process

Trained professionals watching the alerts as they come in 24/7, correlating the alerts with what is already known about your environment, including all available threat intelligence, and providing actionable information as soon as possible after a threat is discovered.



Dell SecureWorks believes security is a business imperative that cannot be solved by technology alone. We help organizations simplify and solve security challenges to reduce business risk and prove measurable outcomes. Elite intelligence developed by our security experts creates a security continuum that ensures you see the threat, stop cyber-attacks, and recover faster from security breaches.

Speak with a Dell SecureWorks Security Specialist today 877-838-7947

DELL SecureWorks

secureworks.com/AMPD
info@secureworks.com
twitter.com/dellsecureworks
facebook.com/secureworks
linkedin.com/company/secureworks