NEW PONEMON INSTITUTE STUDY: KEY FINDINGS

The 2017 State of Endpoint Security Risk

Attacks are evolving.

As a result, today's organizations are struggling to secure their endpoints, and paying a steep cost for each successful attack. To discover how exactly endpoint security is breaking down, and what organizations are doing to fix it, the Ponemon Institute independently surveyed 665 IT security professionals responsible for managing and reducing their organization's security risk.

The findings indicate we are in the midst of a significant shift in endpoint security. Faith in traditional solutions such as antivirus programs that rely on file scanning and signature matching has declined significantly in the face of new, fileless threats. The majority of organizations are replacing or augmenting these solutions with new security tools designed to stop fileless attacks, though many remain skeptical such attacks can be stopped at all.

In addition to reporting a significant rise in the new types of attacks they're seeing, respondents also indicated their organizations are struggling to keep the cost and complexity of managing endpoint security down. False positives were ranked as the most significant "hidden" cost of endpoint protection — nearly half the alerts IT security teams responded to were false alarms. Adding to that management challenge is the fact that organizations now have an average of seven different agents installed on endpoints, with each requiring its own monitoring. Only a third of organizations report having enough resources to effectively manage it all.

In the following summary, we'll provide more details behind these trends by highlighting the top challenges and biggest changes impacting endpoint security today. We'll also reveal the specific types of attacks that are getting past traditional endpoint solutions most often, and break down the true costs of those attacks on victim organizations.

Get the full report

Ponemon INSTITUTE

Barkly

Contact us: **info@barkly.com 617.275.2074**

KEY FINDING #1

Fileless attack techniques are on the rise. Current solutions aren't stopping them.

Seven out of 10 of the respondents surveyed indicated the endpoint security risk to their organization has significantly increased during the past 12 months. Corresponding with that increase is a rise in "fileless" attacks that exploit a fundamental gap in traditional endpoint security.

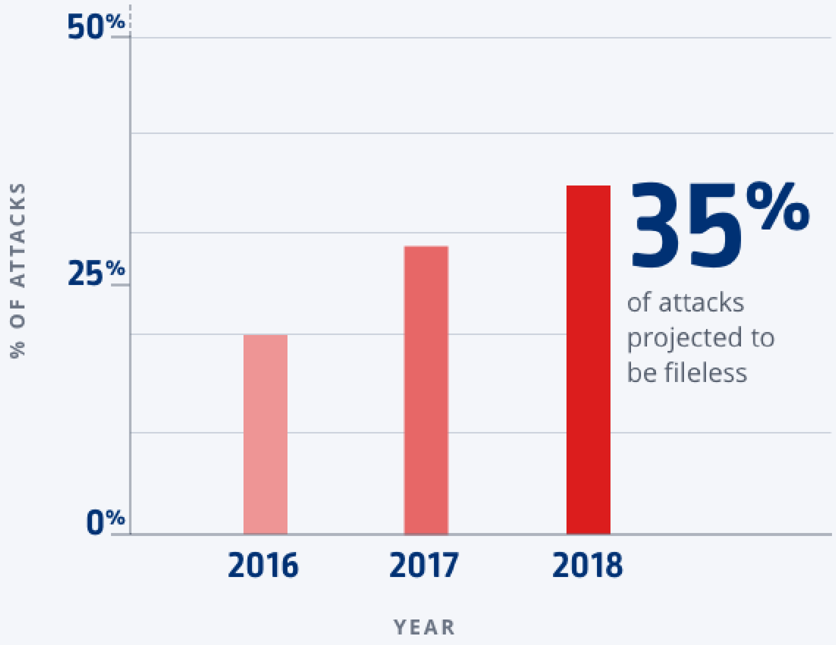
Rather than install malicious executable files that antivirus solutions can scan and block, these attacks instead leverage exploits designed to run malicious code or launch scripts directly from memory, infecting endpoints without leaving easily-discoverable artifacts behind. Once an endpoint has been compromised, these attacks can also abuse legitimate system administration tools and processes to gain persistence, elevate privileges, and spread laterally across the network.

Surveyed organizations estimated 29 percent of the attacks they faced during 2017 were fileless attacks, up from 20 percent the year before. They project that proportion to continue to rise next year, with fileless attacks estimated to make up 35 percent of all attacks in 2018.

What constitutes a fileless attack?

A fileless attack is an attack that avoids downloading malicious executable files at one stage or another by using exploits, macros, scripts, and legitimate system tools, instead.

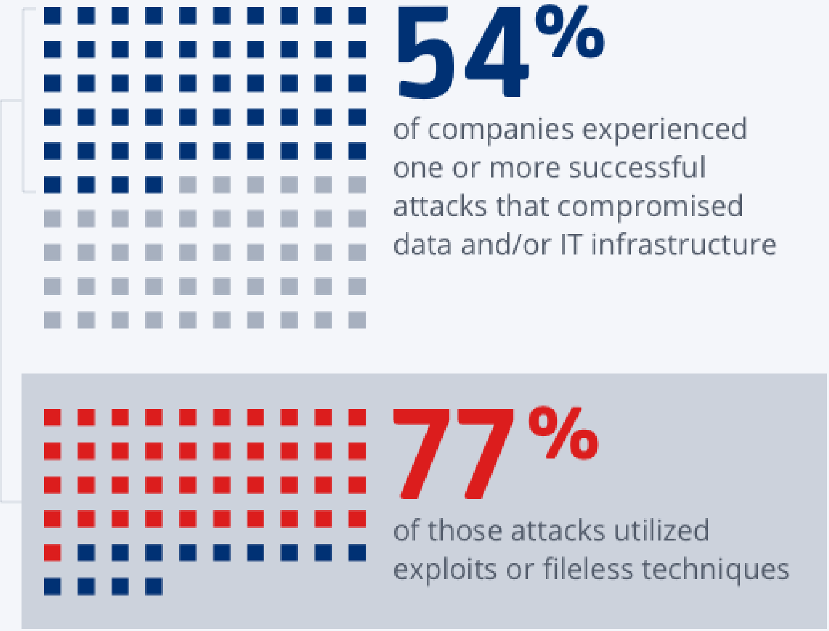
Growth in fileless attacks



Why the uptick? Fileless attacks are working. According to the responses, 42% of companies experienced one or more fileless attacks that successfully compromised their data or IT infrastructure in 2017. In fact, over three-quarters of reported successful compromises involved fileless techniques.

Fileless attacks are almost 10x more likely to succeed than file-based attacks.

The majority of successful attacks are fileless



KEY FINDING #2

Antivirus solutions are being replaced or supplemented.

The success of fileless attacks has further eroded organizations' trust in their existing security solutions. Less than a third of respondents believe their antivirus (AV) can stop the threats they are seeing. As a result, the vast majority are investing in new technology.

One third of respondents reported they had replaced their AV with another vendor's AV or a next-generation endpoint solution. Half of the organizations reported they had and kept their existing AV and added solutions with either additional protection or detection and response capabilities.

4 out of 5 organizations replaced or augmented their existing antivirus solution in 2017.

Despite the addition of new technologies, only 54 percent of survey respondents indicated they believed the attacks they're seeing can be realistically stopped.

KEY FINDING #3

Ransomware is still a major issue.

Ransomware attacks continue to be a major cause for concern, with more than half of the surveyed organizations experiencing one or more ransomware incidents in 2017. Of those organizations, 40 percent experienced multiple ransomware incidents.

Nearly two-thirds (65 percent) of organizations reported having paid a ransom. The average ransom payment was $3,675.

KEY FINDING #4

Endpoint security risk is becoming more difficult and costly to manage.

In addition to failing to stop new attacks, many existing endpoint solutions are also putting an untenable strain on staff, resources, and overall productivity, the respondents report.

Nearly three out of four respondents (73 percent) say it has become more difficult for their organization to effectively manage endpoint risk, with only a third of respondents indicating they have adequate resources to do so.

The average organization has an average of seven different software agents installed on its endpoints to enable IT management and security, making endpoint management noisy and time-consuming.

When asked to identify the biggest problems with their current endpoint solutions, responding to high numbers of false positives and security alerts was listed as the #2 pain point behind "does not provide adequate protection." The third-highest pain point was tied to the complexity of deployment and management, and the fourth-highest was negative impact on user productivity.

Nearly half of all security alerts are false positives, which respondents ranked as the most significant "hidden" cost of endpoint protection.

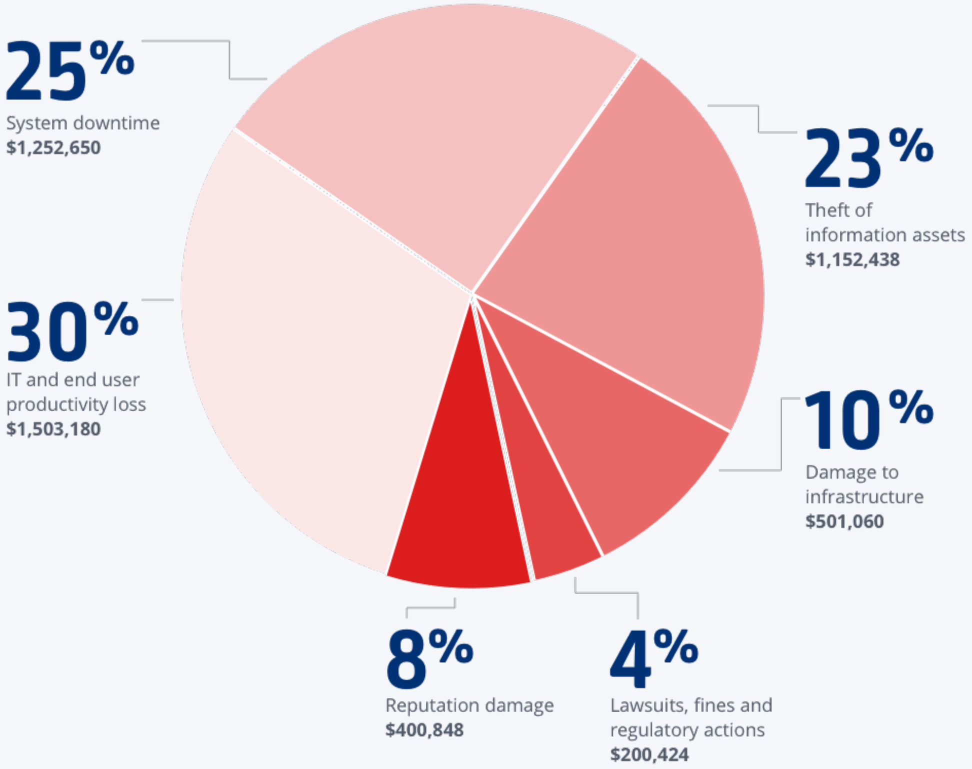
KEY FINDING #5

The total cost of a successful attack is over $5 million.

For the attacks that did get through existing endpoint security, the cost to victim organizations was significant. On average, companies lost a total of $5,010,600 (average cost $301 per employee).

Cost of endpoint attacks

The average organization lost $5,010,600 million due to endpoint attacks in 2017



Conclusion

The current endpoint security solutions organizations are deploying are ineffective at stopping today's new and evolving attacks. In addition, implementation and management of these solutions is placing unjustified strain on organizations' employees and resources.

As a result, many organizations are moving beyond their current antivirus solutions, but the majority are choosing to replace or supplement them with solutions that do not truly address their gaps in protection (e.g. other AVs or endpoint detection and response solutions that mitigate attacks after damage is done).

With the average cost of a successful endpoint attack totalling over $5 million in downtime, damages, and loss of productivity, waiting to address attacks until after they have taken place is untenable.

Based on this research, organizations can clearly benefit from endpoint security solutions designed to block new threats like fileless attacks, which are responsible for the majority of today's endpoint compromises. To restore their faith in endpoint security's effectiveness, new solutions need to address this crucial gap in protection without adding unnecessary complexity to endpoint management.