eset
Internet Security

WHITE PAPER

WHY LAST YEAR'S SECURITY STRATEGY CAN'T PROTECT YOU FROM TODAY'S THREATS

SPRING 2013

Why last year's security strategy can't protect you from today's threats

If you deployed your security solution even just last year, you may not be protected from some of today's most common malware. Today's attacks are more frequent, more devious and more targeted, successfully penetrating many businesses that consider their security strategies to be more than adequate.

Hackers have become methodical and are flooding targets with an overwhelming amount of new malware, using social media sites and "bring your own device" security loopholes to quickly distribute and execute attacks. Criminal and other well-funded organizations are deploying sophisticated threats designed to siphon the bank accounts of unsuspecting small business owners. Fake antivirus referred to as "scareware" imitates legitimate security products to trick users into giving up confidential information or buying rouge security software that doesn't work. Cyber extortionists use "ransomware" to lock users out of their own systems until they pay a ransom – and then refuse to ante up.

> **All of these threats are increasingly targeted towards small to medium-sized businesses that are vulnerable because of their small or nonexistent IT staff, outdated security practices, and backdoors that can be used to infiltrate larger business partners.**

If your security strategy hasn't kept up with this transformation, you could be facing avoidable risks without realizing it. This white paper explains how virus and malware threats are changing and what you can do to protect your business.

Business is booming – and malware is everywhere

In 2012, over 34 million new variations of malware were detected by AV-TEST – an increase of over 88% compared to the previous year. This explosive growth is fueled by numerous factors – financial motivation, the availability of DIY virus modules, easier attack routes through social networks, and BYOD devices in the workplace – all which present exploitation possibilities.

Even as they're rising in scale, attacks are changing in nature. In years past, hackers were generally individuals or small groups looking only for notoriety. Today, criminal coalitions are working together for profit, often supported by organized crime or rogue governments in Eastern Europe and the Middle East. This support allows them to invest significant amounts in advanced tools that let them more easily evade detection and find vulnerabilities in single layer security solutions.

In 2012, over

34 million

new variations of malware were detected by AV-TEST

Evasive new threats require a new strategy: Seven trends to watch

Cybercriminals are getting smarter and businesses must change their strategies to adapt to how today's threats are distributed.

Businesses should be aware of the following trends when evaluating their security strategy and software:

1. Distribution via document sharing

Organized hackers have generally moved away from the use of self-replicating malware. They are instead spreading attacks through PDFs and Microsoft Office documents compromised with zero-day exploits, distributed through network shares, email and infected USB drives.

2. Silent, industrially-focused malware

One of the most recent and sophisticated threats is Stuxnet, which seeks out specific types of industrial systems with code aimed at disrupting or even destroying them. Stuxnet issued commands that damaged uranium centrifuges used by the Iranian government. Its ability to penetrate corporate networks and circumvent traditional security parameters has provided hackers with a new blueprint for virus releases. One toolkit based on this blueprint focuses on zero-day exploits found in the supervisory control and data acquisition (SCADA) controls that are consistently cited as the Achilles' heel of power grid cybersecurity.

3. Stolen SSL certificates

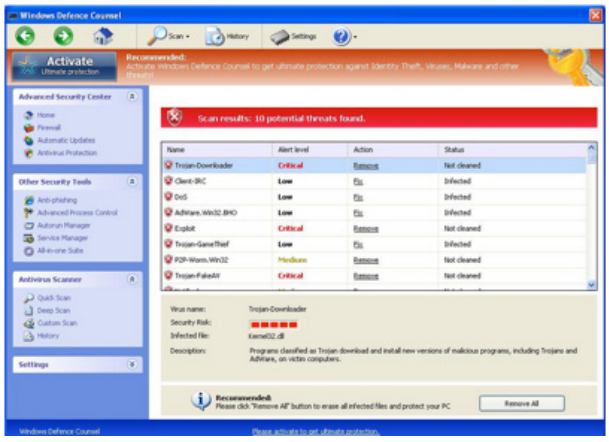
Attackers can utilize stolen digital certificates to intercept encrypted communication and impersonate websites without your knowledge. Credentials gathered during these attacks can be used at a later date on other websites where more sensitive or financial information is stored.

4. Object-oriented malware and code-packing to evade detection

Malware developers have started to utilize complex code packing, obfuscating their attack's true capabilities and allowing them to exist within what appear to be normal programs Another new technique to hide virus signatures and prevent detection is the use of object-oriented programming. The Flame virus is among those that conceals individual virus elements within larger code objects to prevent their detection. All of these trends raise the risk of "zero-day" threats (that exploit a vulnerability the same day it becomes generally known) remaining unlisted in databases of malware signatures, leaving businesses open to attack.

5. DDoS attacks to stop business operations

A growing number of attacks target smaller companies with Distributed Denial of Service (DDoS) attacks. As larger companies get better at defending against them and the cost of mounting such attacks fall, cybercriminals are finding SMBs, and specifically those that do a majority of their business online, to be the ideal target. Many businesses who experience DDoS attacks report they are preceded by a threat to wire money immediately or face indefinite downtime for their website.



"Scareware" attempts to trick users into installing unneeded software.

6. Malware masquerading as legitimate software

Yet another trend is "lookalike" attacks that mimic Windows Control Panel interface features, tricking users into disclosing personal information or purchasing fake antivirus or other faux-security software.

7. SEO poisoning

Hackers are utilizing "SEO poisoning" that targets susceptible users searching for popular or "trending" phrases and manipulates search engine results to direct them to sites that will perform a "drive-by" download of malware. That code then gathers personal information, or silently takes control of that computer for use as part of a larger botnet attack.

The new target: Top 3 SMB security vulnerabilities

Many SMBs underestimate the security dangers they face in today's threat environment. Eight out of ten small business owners believe it is unlikely they'll suffer a data breach, and fail to take even basic measures to secure sensitive data, according to a recent survey performed by The Hartford Insurance Company.[1] Many businesses have little training in or understanding of laws governing how personally identifiable information should be encrypted, shared, or stored and lack policies ensuring their staff complies with those requirements.

These same businesses often rely on single-layer security solutions, such as standalone antivirus software, which leave them open to attack if their defense is breached. Hackers are more likely than ever to target SMBs, hoping their lack of preparation and limited security expertise will make it easy to penetrate their systems and those of their business partners. SMB business owners should correct these vulnerabilities to keep themselves protected:

1. Reliance on signature databases, not heuristics

A fundamental flaw is that many traditional antivirus products compare the files on a user's system to only a limited library of known bad signatures, or look for only exact matches with such signatures. Many that do not perform advanced heuristic analysis (examining the structure or behavior of suspicious code) have difficulty detecting malware that is released in many subtle variations or morph every few hours to evade signature-based detection, a common practice for today's developer.

2. Only one line of defense against malware

Many SMB security plans are comprised of only a single product, usually antivirus, and do not include an advanced firewall to block and flag suspicious network traffic or have separate protection for other endpoints such as email and servers. Furthermore, for companies that allow employees to BYOD, these personal devices can be an attack route into the corporate network if users download malware disguised as legitimate applications, or fail to run antivirus software at all. Having the capability to lock down specific USB ports is essential.

3. Social media access at work leaves businesses vulnerable to viral attacks

Attackers are using the viral aspect of social media (and the unsuspecting and trusting nature of many users) to speed viruses around the globe more quickly than ever. By convincing one user to share an infected file or link with their network (or simply crack the credentials for an account), attackers can exploit personal connections for profit.

Older security strategies may have been adequate when there were fewer threats, less sophisticated attack models and more time to adjust defenses to new attacks. Today's advanced threats expose the weaknesses of these older strategies and leave little room for error.

[1] The Hartford Small Business Data Protection Survey, June 6, 2012.
http://newsroom.thehartford.com/News-Releases/Small-Business-Owners-mdash-Despite-Being-Increasingly-Targeted-mdash-Believe-Data-Breach-Unlikely-50c.aspx

Modern threats need modern protection

Even if your security solution is only a few years old, you may be a target. Just because you're a small business doesn't mean you (or your business partners) can't be ruined by hackers. Protect your finances, your brand, your reputation, and your relationships with a security solution that protects you from today's complex, fast-changing threats against SMBs.

About ESET

ESET is a global leader in antivirus and Internet security software with 25 years of proven experience. Powered by ESET NOD32® technology, which has won an unmatched 76 VB100 awards for malware detection, ESET business solutions offer proactive, fast, and effective server-to-endpoint protection for PC, Mac and mobile-based environments. **Proven. Trusted**

ESET: Modern protection against modern threats

ESET's business security suite is engineered to find the most recent threats, even those whose signatures have not yet appeared on known malware lists, that are disguised as legitimate software or that are hidden within larger blocks of code.

With its powerful and award-wining NOD32® technology, now in its fifth generation, ESET's security software uses advanced heuristics to find and block codes or signatures even if they are not an exact copy of known malware. It does this by monitoring the structure and behavior of suspicious code within your systems in real-time, 24 hours a day and 365 days a year.

As a secondary layer of protection, ESET's Live Grid provides validation of scanned items and determines known good files based on the analysis of anonymous system scans from more than 100 million ESET users worldwide. This cloud database is synchronized with each new signature update and locally correlates a file's reputation ranking based on data collected from LiveGrid. Because ESET's customers are truly global, LiveGrid finds and stops more viruses and malware than other vendors who have customer bases in fewer regions.

To ensure you are protected against the latest threats, ESET doesn't wait for major release cycles to distribute product updates to customers. It instead continually publishes product module updates, making them part of regular virus signature definition upgrades when appropriate. This combination of technology and best practices is why, in independent tests conducted by AV Comparatives, ESET has never failed to discover a virus "in the wild."

ESET also provides layers of protection for servers, endpoints and email. This protects against infection that may touch more than one location and ensures that the breach of a single platform doesn't let malware infect your entire IT infrastructure.

To learn more about ESET endpoint solutions or for a free trial, visit www.eset.com/us/business