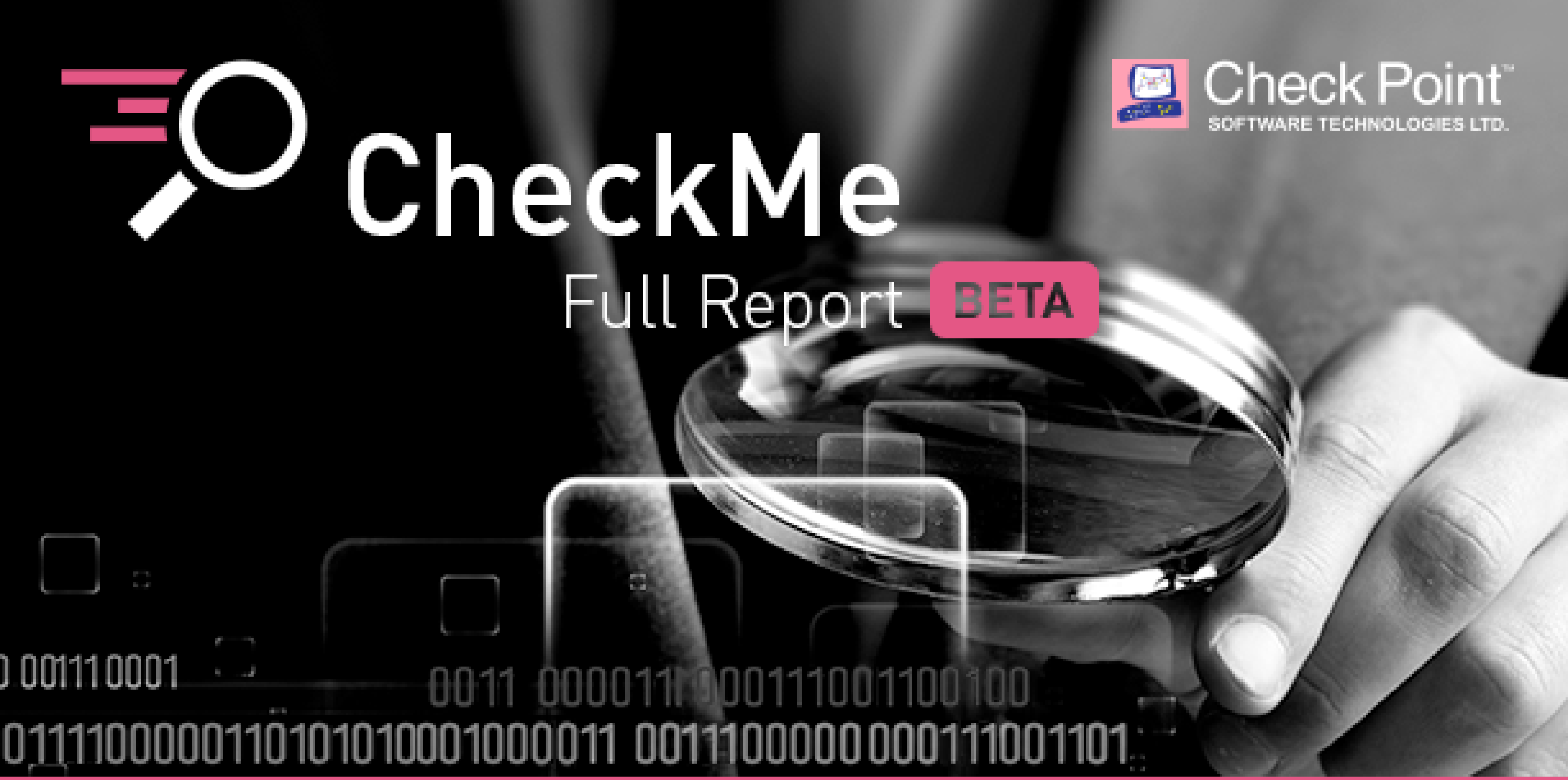


Check Point™ SOFTWARE TECHNOLOGIES LTD.

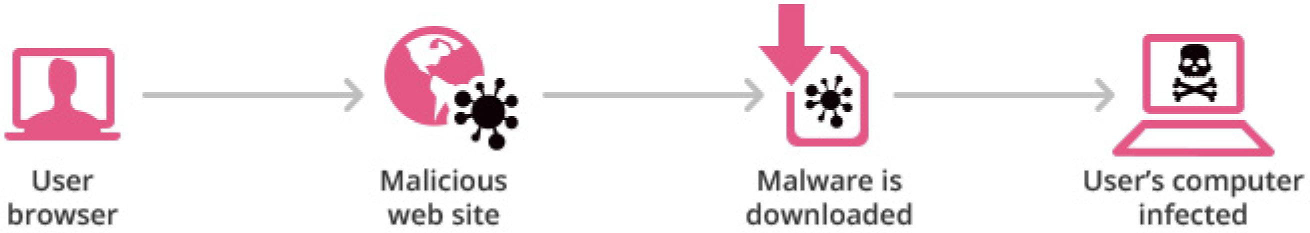
CheckMe

Full Report BETA

On an average day, users download malware every 81 seconds. They access malicious websites every 5 minutes. Threat actors release 1 million new forms of malware every day. These all add up to a significant likelihood your network will be breached.

ARE YOU VULNERABLE TO NEW TYPES OF ATTACKS?

CheckMe simulates many types of attacks that can compromise your computer and the information on your network. This report summarizes your computer's vulnerability to ransomware, phishing, zero-day malware, bot infections, data leakage, and other threats.



©2017 Check Point SOFTWARE TECHNOLOGIES LTD.
All rights reserved.

EXECUTIVE SUMMARY

✓ 06 Tests SECURED

✗ 01 Tests VULNERABLE

IP Address	Assessment Date	Operating System Family
194.29.33.48	February 5, 2017	Windows

The following report presents your network exposure to top security threats as:

✗ **IDENTITY THEFT / PHISHING** attack captures personal information by fake websites that appears to be legitimate.

✓ **RANSOMWARE** is a type of malware that encrypts users' files and require ransom for their decryption.

✓ **ZERO DAY** attacks use the element of surprise and exploit a hole in the software that is unknown to the vendor.

✓ **BOTS** perform malicious attacks that let attackers take complete control over an infected computer.

✓ **BROWSER ATTACKS** inject malicious script into websites to steal cookies from victims for the purpose of impersonating the victims.

✓ **ANONYMOUS** surfing allows users to hide their online activity. It can open backdoors into an organization's network.

✓ **DATA LEAKAGE** is the transfer of classified or sensitive information outside an organization's network by theft or accidental exposure.

©2017 Check Point SOFTWARE TECHNOLOGIES LTD.
All rights reserved.

REPORT RESULTS

Identity Theft / Phishing

Threat actors primarily use phishing sites to gather sensitive information. They use this information either to directly impact the individual connecting to the site, such as bank customers, or to conduct follow-up attacks, for example gathering administrator credentials.

This test generates connections to phishing and malicious sites. A successful communication attempt is an indication that you could fall prey to a phishing attack and your personal information could be stolen. For more information click here.

✗	Simulating connection to phishing sites.
✓	Simulating connection to malicious sites.

Remediation

Blocking phishing attacks requires URL Filtering protection, which is an integral component of Check Point's Next Generation Threat Prevention (NGTP) and Next Generation Threat Extraction (NGTX) solutions, can be used to block connections to known phishing sites.

Ensure that phishing and high risk categories are configured in prevent mode within the URL Filtering policy to protect your computer from this threat.

©2017 Check Point SOFTWARE TECHNOLOGIES LTD.
All rights reserved.

Ransomware

Ransomware is a form of malware that has grown in frequency and severity. This malware encrypts files, making them unusable. Ransomware forces users to purchase keys to decrypt the files.

To bypass traditional anti-malware solutions, attackers will often package their exploits within standard document formats as well as more complex vehicles such as compressed archives, or through encrypted file distribution channels. This test attempts to download files in different formats and containing malicious attributes that are often used in ransomware attacks. For more information click here.

- ✓ Downloading of infected file through your network.
- ✓ Downloading of infected zipped file through your network.
- ✓ Downloading of infected file through your network over HTTPS.
- ✓ Downloading a file that reveal your expusure to IE8 exploit.

©2017 Check Point SOFTWARE TECHNOLOGIES LTD.
All rights reserved.

Zero Day Vulnerability

Cyber threats are continuing to evolve. Hackers are finding new ways to hide malware inside emailed documents, on websites as “drive by” exploits or in downloadable content. Many attacks begin by exploiting known vulnerabilities and modifying malware to have unrecognizable signatures to evade traditional security measures. By creating these new, unknown variants, hackers aim to avoid detection by signature-based security solutions, to breach the network and steal critical information.

This test attempts to download files in different formats that are often used in Zero Day attacks. For more information click here.

✓	Downloading an Infected PDF file with random suffix (hide the real format of the file) through your network.
✓	Downloading of an archive with infected PDF file through your network.
✓	Downloading of an infected PDF file through your network.

©2017 Check Point SOFTWARE TECHNOLOGIES LTD.
All rights reserved.

Bot Infection

Malware refers to software that is intentionally designed to be malicious. Over the past few years malware has morphed into tools that are developed and used by a wide range of professional threat actors, such as organized crime rings or agents sponsored by nation-states.

The final phase of malware-based attacks is the use of command and control sites for remote administration of the malware. This test generates requests to known command and control servers. For more information click here here.

✓	Simulating command and control communication to external server.

©2017 Check Point SOFTWARE TECHNOLOGIES LTD.
All rights reserved.

Browser Attack

This test included the use of cross-site scripting (XSS). Such attacks can be used to inject malicious content from an infected site onto the user's machine via their browser. This attack is often used in websites where user input is gathered without validation or encoding.

This test runs a connection attempt to a site that is known to contain malicious content that can be injected into a browser. For more information click here.

✓ Simulating access to a website that can be infected with java script code.

©2017 Check Point SOFTWARE TECHNOLOGIES LTD.
All rights reserved.

Anonymizer Usage

The use of Anonymizers has many security implications. It shows that users are hiding their online activity. Anonymizers also indicate potential coordinated campaign activity. Attackers often coordinate their efforts through encrypted communications channels. Further, instructions for the use and purchase of attack tools are often only available on marketplaces within the Dark Web. These sites can only be accessed with anonymizers.

This test generates connections to anonymizers. For more information click here.

✓	Simulating access to an anonymizing site that allows users to hide their online activity.

©2017 Check Point SOFTWARE TECHNOLOGIES LTD.
All rights reserved.

Sensitive Data leakage

Data leakage happens when users transfer classified or sensitive information outside the corporate network purposely or by mistake. In contrast, exfiltration is the deliberate extraction of sensitive data by external parties. Both are dangerous and can lead to the loss of customer and company sensitive information such as financial data and credit card data. These risks are often the final phase of a security breach. Data leakage and exfiltration can also violate regulations and industry guidelines such as PCI DSS.

This test attempts to upload payment card data to public websites. For more information click here.

✓	Posting credit card numbers to external sites over http.
✓	Posting credit card numbers to external sites over https.

©2017 Check Point SOFTWARE TECHNOLOGIES LTD.
All rights reserved.

CONCLUSIONS

CheckMe checked your exposure to 7 common threats based on series of tests that were simulated on your computer and network. The assessment found that you are exposed to 1 threat.

Mitigating attacks like these requires a security strategy that coordinates multiple protections in a preventative approach. Preventative methodology is the foundation of the Check Point solution set. Our solutions (NGTP, NGTX, SandBlast, Endpoint) integrate multiple levels of protections into unified security platforms. In addition, our unified management architecture empowers administrators to build policies and analyze events across all solutions efficiently and effectively.

This CheckMe report is a single snapshot of your security profile. Check Point offers consulting services that can provide you with a full view of your current security profile. We can help you understand how you are positioned today and use this understanding to build a path with that will let you to improve your posture going forward.

For more information on Check Point technologies and services please contact your local partner and account team or find us online at

https://www.checkpoint.com/about-us/contact-us/

CONTACT US

©2017 Check Point SOFTWARE TECHNOLOGIES LTD.
All rights reserved.