UNDETECTED CYBER THREATS

An Analysis of Company and Employee Exposure to Contemporary Attacks That Evade Traditional Security

WHITE PAPER

January 2021

ERMES®
Intelligent Anti Phishing

www.ermes.company

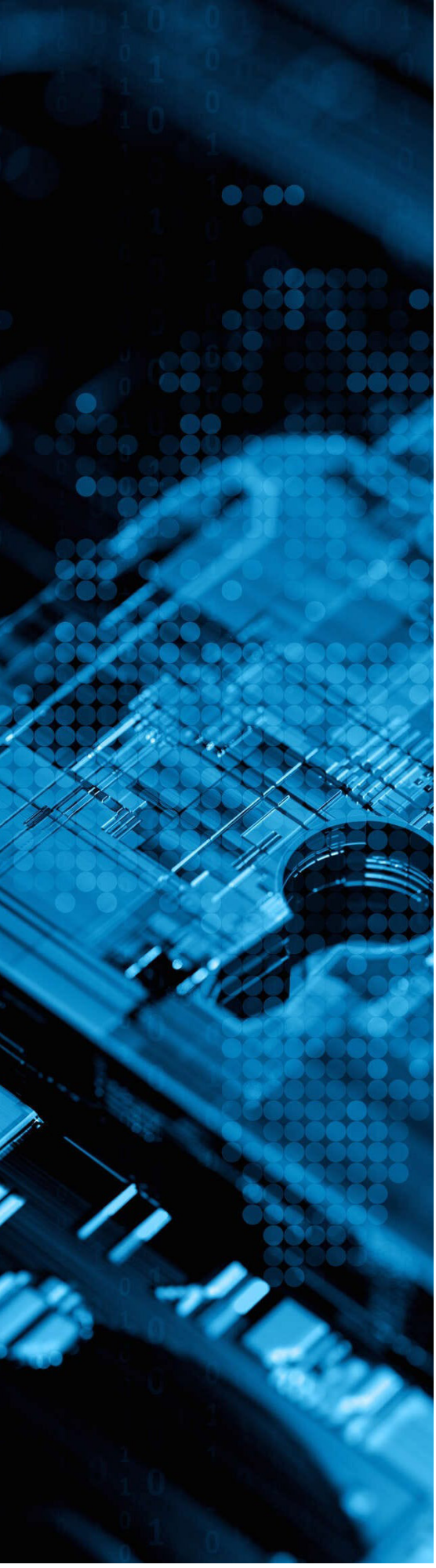
Copyright © 2021 Ermes Cyber Security S.R.L

> It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it.

Stéphane Nappo

Global Head Information Security for Société Générale International Banking pole

Copyright © 2021 Ermes Cyber Security S.R.L



CONTENTS

Copyright © 2021 Ermes Cyber Security S.R.L

1 Executive Summary

This white paper provides an overview of the corporate battle being waged against evolving and sophisticated cybercrime. It also includes the results of in-depth research demonstrating how **existing corporate security solutions in place at most organizations are failing to block connections to many malicious websites** on a daily basis.

The heaviest responsibility for protecting enterprises against these attacks are with Chief Information Security Officers (CISOs), IT managers, and Chief Technology Officers (CTOs) of business organizations or third parties providers of security solutions such as MSPs,[1] System Integrators and others.

These professionals have staked their reputations and careers on preventing cyber breaches from occurring that currently have an average incident cost of $3.92 million. Just even one cyber incident could be catastrophic to a company and a career.

1. MSPs typically provide security solutions to their clients in addition to other services such as infrastructure and productivity software.

Copyright © 2021 Ermes Cyber Security S.R.L

Overview

- Cybercrime is clearly proliferating and occurring everywhere the web reaches, especially in Europe and the U.S. The COVID-19 pandemic has further exacerbated the situation resulting in a surge of incidents due to remote systems and unstable conditions.

- It has been estimated that related damages due to cyber-crime around the globe could reach $6 trillion annually by 2021 according to a report prepared by Cybersecurity Ventures.

- To combat attacks by cyber criminals, Gartner is forecasting that worldwide spending on information and cyber-security could reach $170.4 billion by 2022.

- Contemporary cyber-attacks conducted mostly through web browsers and email have been generally referred to as “phishing attacks.” These attacks involve the practice of sending fraudulent digital communications that appear to come from a reputable source. Data exposed by users during navigation—by contacting web trackers or web keyloggers— are used by malicious entities to prepare and deliver targeted attacks such as malicious browser extensions, tabnabbing, malvertising, cybersquatting, and cryptojacking.

- Many of these threats and attacks remain invisible. Traditional security systems currently in place at organizations such as endpoint protection, network filtering, and endpoint detection and response (EDR) are not enough by themselves to fully detect and block these complex and sophisticated attacks.

- According to research conducted by the Ponemon Institute, artificial intelligence (AI) or a deep-learning-based solution can get better results in the battle against cyber-crime by (1) lowering false positive rates, (2) increasing detection rates, and (3) preventing unknown first-seen cyber-attacks.

Copyright © 2021 Ermes Cyber Security S.R.L

Ermes' Research

- **Ermes**–Intelligent Anti Phishing which leverages AI and deep-learning technology by providing an additional layer of protection conducted a study in 2020 to evaluate the effectiveness of exclusively relying on traditional corporate security solutions to identify and block malicious websites.

- **Ermes** conducted a study with a representative sample of 13 organizations in a variety of industries that relied solely on traditional security solutions to block malicious websites. A total of 361 employees participated with an average of 28 per company. For each of these employees **Ermes** installed its software solution on their devices and analyzed **86,754,580 connections** for cyber threats.

+86M
connections analyzed

- Overall, **Ermes** found that **91.97% of the employees participating in the study had their data exposed to web tracking** systems even with traditional corporate solutions in place.

- **74.38%** of the domains visited by these employees were also tracked.

- A total of **139,783** -page titles and **33,026** search queries were exposed to third-party systems potentially providing cyber criminals with sources of information to build an attack.

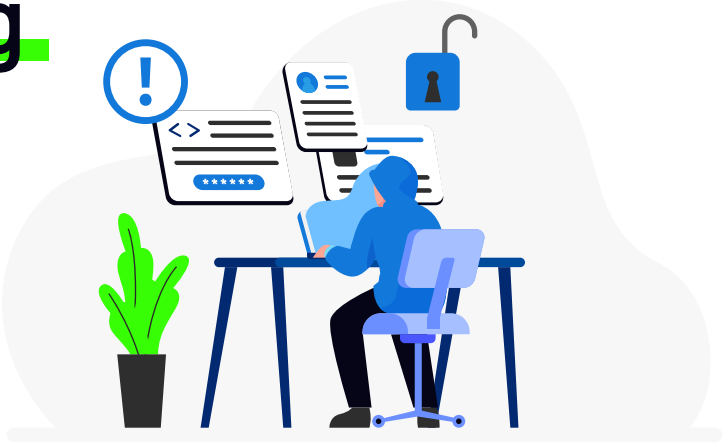
- **Ermes** observed that exposure to the contemporary cyber threats is spread across all types of organizations regardless of industry or size.

- **93.2% of attempts to reach malicious website were not blocked by traditional security systems.**

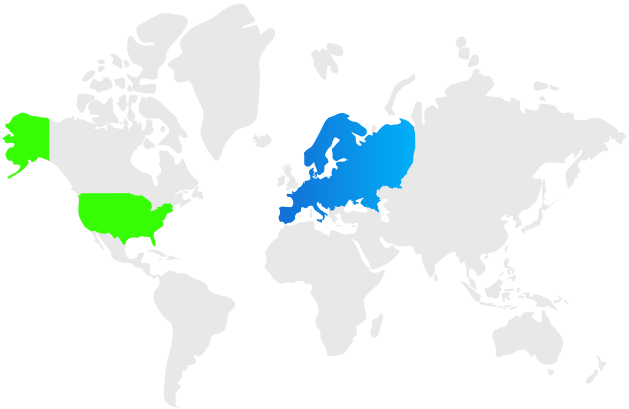
- **4.09 malicious websites** are visited on average by each employee every year and are not blocked by the traditional corporate security solutions in place.

Copyright © 2021 Ermes Cyber Security S.R.L

2 The Corporate Battle Against Evolving Cyber-Crime



Overview



Cyber-crime has reached epic proportions globally, especially in Europe and the U.S., with related damages to enterprises projected to reach $6 trillion annually by 2021.[2] According to a study conducted by the University of Maryland, there is a cyber-attack once every 39 seconds.[3]

RiskBased Security (RBS)—a firm that provides detailed information and analysis on vulnerability intelligence and data breaches—found that for the first six months of 2019 alone there were 3,813 breaches exposing over 4.1 billion records. Of these, the web was the number one breach type for number of records exposed, accounting for 79% of the compromised records.[4]

Organizations experiencing web-based[5] cyber-attacks may be inadvertently exposing sensitive corporate information that can pose substantial risks and damages. Among these risks and damages are identity theft including digital identity/credential loss, stolen customer credit card data, bank information, and misappropriation of confidential business documents with trade secrets. On top of this, organizations breached by one of the many forms of today's evolving cyber-crime threats may experience crushing

2. See Official Annual Cybercrime Report, dated October 26, 2020, prepared by Cybersecurity Ventures at https://cybersecurityventures.com/annual-cybercrime-report-2020/. According to the report, cyber-crime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems as well as reputational harm. The damage cost estimation is based on historical cyber-crime figures including recent year-over-year growth, a dramatic increase in hostile nation-state sponsored and organized crime gang hacking activities, and a cyber-attack surface which will be an order of magnitude greater in 2021 than five years ago.

3. See study conducted by Assistant Professor Michel Cukier of the Clark School's Center for Risk and Reliability Institute for Systems Research, University of Maryland at https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds.

4. See Cyber Risk Analytics (CRA), 2019 MidYear QuickView Data Breach Report, RiskBased Security, issued August 2019 at https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report.

5. This is even more pronounced because navigation is typically not protected which can result in sensitive data being exposed leading to a data breach.

Copyright © 2021 Ermes Cyber Security S.R.L

damages for legal liability and compliance violations along with severe reputational harm that may not ever be fully recoverable.

A study by Verizon indicated that 86% of breaches were financially motivated while 10% were the result of espionage.[6] This same study found that credential theft, social attacks (i.e., phishing and business email compromise), and errors cause the majority of breaches (67% or more). Because these tactics prove effective for attackers, they return to them time and again. Accordingly, for most organizations, these three tactics should be the focus of the bulk of security efforts.[7]

To combat attacks by cyber criminals, Gartner has reported that worldwide spending on information and cyber-security would reach $123.8 billion in 2020.[8] This same market is now forecasted by Gartner to increase to $170.4 billion in spending by 2022.[9] These costs reflect the ever expanding cyber-security threats that have morphed into a day-to-day battle for businesses with the heaviest responsibility clearly landing on Chief Information Security Officers (CISOs), IT managers and Chief Technology Officers (CTOs) of companies.

These professionals not only have full accountability for securing their organization's critical systems against malicious data breaches—that currently have an **average incident/breach cost of $3.92 million**[10] but they have also staked their own reputations and careers on preventing it from ever happening. While a CISO can leave a position for any number of reasons, a breach or other security incident may very well hasten that.[11]

Cyber-crime is clearly proliferating and occurring everywhere the web reaches, especially in Europe and the U.S. **Since 2000, the use of online technologies for both the working environment and society at large has dramatically evolved to meet changing conditions.** The COVID-19 pandemic has only accelerated these trends that were already in place and further exacerbated the situation resulting in a surge of incidents due to unstable conditions.

6. See 2020 Data Breach Investigations Report (DBIR), Verizon, page 6 at https://enterprise.verizon.com/resources/executivebriefs/2020-dbir-executive-brief.pdf.

7. Ibid.

8. See "Gartner Forecasts Worldwide Security and Risk Management Spending Growth to Slow but Remain Positive in 2020," dated June 17, 2020 at https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem.

9. See "Forecast Analysis: Information Security, Worldwide, 2Q18 Update," Gartner, dated September 14, 2018 at https://www.gartner.com/en/documents/3889055.

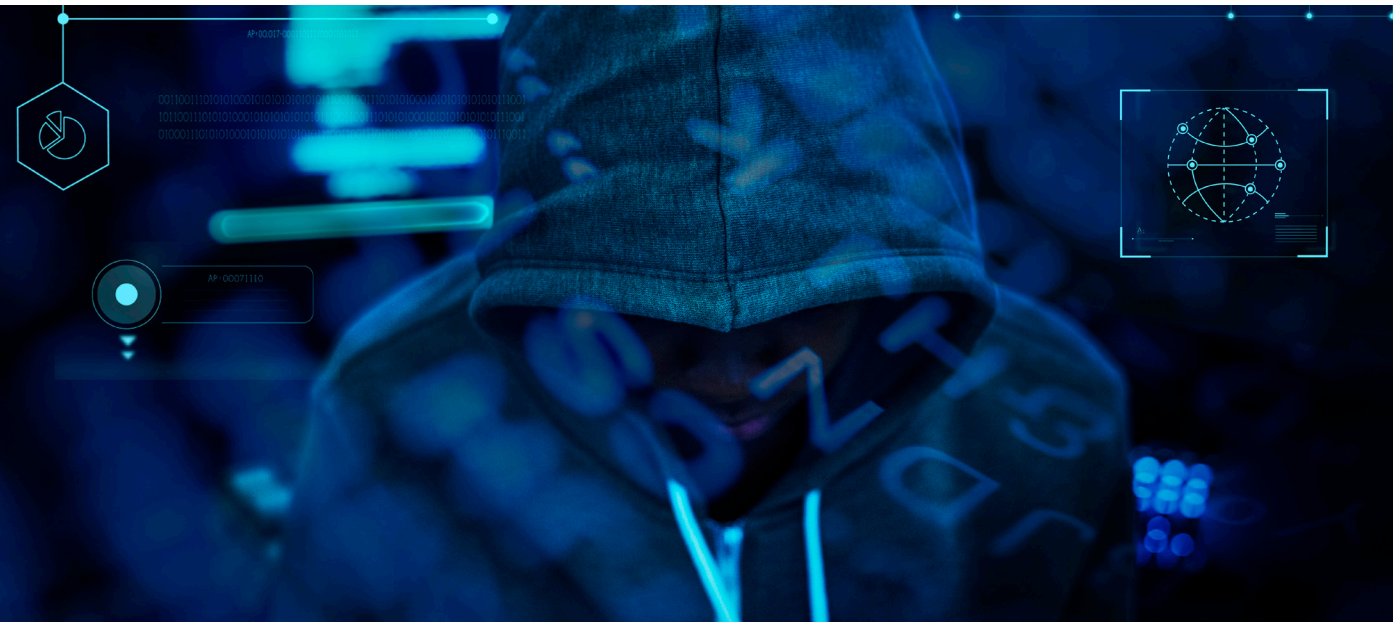
10. See "What's New in the 2019 Cost of a Data Breach Report," Security Intelligence, dated July 23, 2019 at https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/.

11. According to Radware's 2018 State of Web Application Security report, 23% of companies reported executive firings related to application attacks. A Nominet survey of over 400 CISOs in the U.S. and U.K. conducted by Osterman Research found that 6.8% of CISOs in the U.S. and 10% in U.K. believed that in the event of a breach they would lose their job. Just under 30% of survey respondents believed they would get an official warning. See "7 Security Incidents That Cost CISOs Their Jobs," CSO, dated January 2, 2020 at https://www.csoonline.com/article/3510640/7-security-incidents-that-cost-cisos-their-jobs.html.

Copyright © 2021 Ermes Cyber Security S.R.L

These incidents stemmed from organizations and businesses rapidly deploying remote systems and networks to support staff working from home. Accordingly, cyber criminals are taking full advantage of increased security vulnerabilities to steal data, generate profits, and cause disruption. Jürgen Stock, the Secretary General of the International Police (INTERPOL) recently said, "Cyber-criminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19."[12] Furthermore, because attackers always exploit trending interests and current societal vulnerabilities, it is safe to assume that 2021 and beyond will present a new set of changes and challenges that will attract cyber criminals in much the same way as COVID-19 did.

In 2019, the number of cyber-attacks reported to Italy's Computer Emergency Response Team (CERT)[13] were 6,211 incidents. Of these, phishing (3,450) and malware (2,040) represented the top two attack methods.[14] Furthermore, in the past several years there have been notable cyber-attacks and data breaches in the U.S. that targeted several high-profile companies. Each had devastating consequences and, in several cases, resulted in the termination of the CISO.



12. An INTERPOL assessment of the impact of COVID-19 on cyber-crime has shown a significant target shift from individuals and small businesses to major corporations, governments, and critical infrastructure. In one four-month period (January to April) some 907,000 spam messages, 737 incidents related to malware, and 48,000 malicious URLs–all related to COVID-19–were detected by one of INTERPOL's private sector partners. See "INTERPOL Report Shows Alarming Rate of Cyberattacks During COVID-19," INTERPOL, August 4 2020 at https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.

13. The Italian authority CERT Nazionale operates mainly as a "facilitator" for the solution of cyber incidents at national and transnational level and receives daily reports of incidents related to Italian networks.

14. These statistics were reported on Statista at https://www.statista.com/statistics/649297/cyberattacks-distribution-share-by-method-in-italy-timeline/.

Copyright © 2021 Ermes Cyber Security S.R.L

These included Capital One (2019),[15] Equifax 2017),[16] Uber (2017),[17] Facebook (2018),[18] Target (2014),[19] JP Morgan (2014),[20] and LinkedIn.[21] These breaches, while highly publicized, represent only the tip of the iceberg in terms of the number of attacks on organizations occurring around the world.

15. In July 2019, Capital One announced an attacker had gained access to the personal information of over 100 million customers. The bank learned of the attack months after the fact thanks to a tip-off from a security researcher. Ibid.

16. During 2017, Equifax was compromised via an unpatched consumer complaint web portal. This led to some 143 million customer records–including names, addresses, dates of birth, Social Security numbers, and driver license numbers–being stolen. As well as a lack of patching, the attack went undetected for months due to the company's failure to update a certificate on an internal security tool. The cost of the incident was estimated to be $1.35 billion. The company paid $575 million (potentially rising to $700 million) with the Federal Trade Commission and others. Ibid.

17. In late 2017, ride-hailing company Uber revealed that the data of 57 million riders and drivers had been stolen, including names, email addresses, phone numbers, and driver license numbers. Attackers reportedly accessed Uber's private GitHub code repository–which the company has since admitted did not have multifactor authentication enabled–and used login credentials stored there. Ibid.

18. The Facebook–Cambridge Analytica data scandal was a political scandal in which the personal data of millions of Facebook users were acquired without their consent by British consulting firm Cambridge Analytica, predominantly to be used for political advertising. The data were collected through an app which harvested the data of up to 87 million Facebook profiles. Information about the data use was disclosed in 2018. See "Facebook–Cambridge Analytica Data Scandal," Wikipedia at https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal.

19. The 2014 attack on U.S. retailer Target was one of the most notable cases of a successful supply chain attack—hackers exploited poor security in a vendor to compromise Target's payment systems and steal the payment details of some 40 million customers attack over the Christmas period in 2013. See "7 Security Incidents That Cost CISOs Their Jobs," CSO, dated January 2, 2020 at https://www.csoonline.com/article/3510640/7-security-incidents-that-cost-cisos-their-jobs.html.

20. JP Morgan had a massive breach in 2014 that compromised over 83 million financial accounts in the U.S., including names, email, postal addresses, and phone numbers. Ibid.

21. LinkedIn, the social networking website, was hacked on June 5, 2012, and passwords for nearly 6.5 million user accounts were stolen by Russian cybercriminals. Owners of the hacked accounts were no longer able to access their accounts. In May 2016, LinkedIn discovered an additional 100 million email addresses and hashed passwords that claimed to be additional data from the same 2012 breach. See "2012 LinkedIn Hack," Wikipedia at https://en.wikipedia.org/wiki/2012_LinkedIn_hack.

Copyright © 2021 Ermes Cyber Security S.R.L

The Evolution of Cyber-Crime and New Methods of Attack

Not surprisingly, the history of cyber-crime coincides closely with the evolution of the Internet itself. The first major wave of crime came with the proliferation of email during the late 80s that allowed for a host of scams and malware to be delivered to an inbox.[22] This was followed by the next wave in cyber-crime resulting from the advancement of web browsers during the 90s. At the time, there were a multitude of early generation browsers that were extremely vulnerable to viruses delivered by questionable websites.[23]

However, cyber-crime really began to rapidly accelerate in the 2000s with the emergence of social media. The large numbers of people providing information to databases capturing profile details allowed for a flood of personal information to become vulnerable resulting in a significant rise in ID theft. Online thieves used the information in a variety of ways that included accessing bank accounts and setting up fraudulent credit cards along with other highly creative financial fraud schemes.[24]

Just like the evolution of technology, cyber-crime must also morph to survive. This is why cyber-criminals are constantly creating new attacks types to fit new trends while at the same time tweaking existing attacks to avoid detection.[25] This has ultimately led to several contemporary threats conducted mostly through web browsers that have been generally referred to as "phishing" attacks.

In general, phishing attacks are the practice of sending fraudulent digital communications that appear to come from a reputable source. It is usually performed through a web browser or email. Ultimately, the goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine that can track, snoop, or use unauthorized resources to mine cryptocurrencies. Ransomware can also be installed resulting in threats to publish a company's sensitive data or to entirely block access to it until a ransom is paid.

22. See "Where Does Cybercrime Come From? The Origin and Evolution of Cybercrime," Le VPN, dated October 18, 2018 at https://www.le-vpn.com/history-cyber-crime-origin-evolution/.

23. Ibid.

24. Ibid.

25. See "The Evolution of Cybercrime," Webroot, dated April 23, 2019 at https://www.webroot.com/blog/2019/04/23/the-evolution-of-cybercrime/.

Copyright © 2021 Ermes Cyber Security S.R.L

These types of attacks, while already prevalent, have significantly surged since the onset of the COVID-19 pandemic and quarantine. In just the first quarter of 2020, Google has reported a 350% increase in the number of phishing sites it has identified.[26] In the 2020 Phishing Landscape Report prepared by Cybersecurity Insiders it was noted as a key finding that on average, organizations in their survey are remediating 1,185 phishing attacks every month with an average of 40 each day.[27]

Below is a table summarizing, by type, several contemporary threats that companies and employees are routinely being exposed to through the use of web browsers, email, and messaging apps on computers and mobile devices.

Targeted attacks[28] have a higher percentage of success because they are tailor made by retrieving information through web tracking, keylogging, and browser vulnerability snooping. This information is then used to build a full attack using malicious browser extensions, tabnabbing, malvertising, cybersquatting, and cryptomining.

CONTEMPORARY CYBER THREATS

Type	Description
Web Tracking	Web trackers create digital identities that malicious actors steal to design and plan targeted attacks.
Browser Vulnerability Snooping	Attackers search for outdated software or vulnerable pieces of software installed on user devices in order to exploit them during an attack.
Web Keylogging	Session replay scripts (web keyloggers) are services specializing in tracking any action a user performs on a web page. This might be a mouse click or filling out a form. Collected data may contain sensitive personal information, credentials, or credit card numbers.[29]

26. See "Phishing Attacks Increase 350 Percent Amid COVID-19 Quarantine," PC Magazine, dated March 30, 2020 at https://www.pcmag.com/news/phishing-attacks-increase-350-percent-amid-covid-19-quarantine.

27. See "2020 Phishing Landscape Report," prepared by Cybersecurity Insiders at https://info.greathorn.com/hubfs/2020-Phishing-Attack-Landscape-Report-GreatHorn_1.6.pdf.

28. Targeted attacks are comprised of two main phases: (1) Preparation which includes the studying of the target through web tracking, web keylogging, and vulnerability snooping; and (2) Execution or the "real" attack that includes tabnabbing, malicious extensions, malvertising, cybersquatting, and cryptomining. Please note that web tracking and keylogging may also have some legitimate purposes that are part of the Internet revenue model; however, they can certainly pose a threat when used maliciously.

29. See "No boundaries: Exfiltration of Personal Data by Session-Replay Scripts," Freedom to Tinker, dated November 15, 2017 at https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.

Copyright © 2021 Ermes Cyber Security S.R.L

CONTEMPORARY CYBER THREATS

Type	Description
Malicious Browser Extensions	Browser extensions are pieces of software which allow for browser customization and provisioning of extra browsing functionalities. These browser extensions might be malicious—even if provided by official extension stores. They might contain risky patterns, collect data for unknown purposes, execute arbitrary code hosted on a private website, or be built on top of vulnerable code libraries.
Tabnabbing	This is a phishing technique which changes the context of inactive browser tabs to fool the user.
Malvertising	Malvertising leverages online advertising bids to spread malware.
Cybersquatting	This is a technique at the base of modern phishing. It consists of registering Internet domains similar to legitimate ones associated with popular brands with the intent of surreptitiously attracting users to a spoofed or other site.
Cryptojacking	This type of attack involves JavaScript deployed on web sites intending to exploit the user's browser and computational resources for the purposes of earning large amounts of money by mining cryptocurrency.[30]

30. This practice known as cryptocurrency mining or just cryptomining uses the unauthorized processing power of computers to solve complex mathematical problems and verify cybercurrency transactions. The miners are then rewarded with a small amount of cybercurrency.

Copyright © 2021 Ermes Cyber Security S.R.L

Why Traditional Security is No Longer Enough to Prevent Cyber-Based Attacks

While much technological progress has been made in the ongoing corporate battle against cyber-crime, traditional security systems such as endpoint protection; network filtering; and endpoint detection and response (EDR) are not enough by themselves to fully detect and block the types of complex attacks discussed above that are trending and proliferating at prodigious rates. Many of these threats and attacks remain invisible to the traditional security that is currently in place with many organizations today.

Ermes–Intelligent Anti Phishing builds breakthrough technologies to protect companies against modern web threats on PC and mobile devices leveraging AI and deep-learning. According to recent research conducted by the Ponemon Institute on the economic value of protection in the cybersecurity lifecycle, a deep-learning-based-solution does all the following:

1. lowers false positive rates,
2. increases detection rates, and
3. prevents unknown first-seen cyber-attacks.[31]

To that end, Ermes fully exploits AI and deep-learning technology to effectively protect companies and employees from evolving cyber-attacks in a way that traditional security is unable to effectively do. Basically, this solution provides an additional layer of protection and privacy against web-based vulnerabilities and modern threats that are always evolving and frequently go undetected by traditional corporate security software.

31. See "The Economic Value of Protection in the Cybersecurity Lifecycle," a study conducted by the Ponemon Institute, March 2020, page 3 at https://info.deepinstinct.com/value-of-prevention.

Copyright © 2021 Ermes Cyber Security S.R.L

3 Methodology of Research

In order to show the effectiveness of AI and deep-learning in the battle against cyber-crime, Ermes recently conducted research with 13 companies that were using traditional security systems to demonstrate their continued vulnerability to these evolving cyber threats.

What follows is the specific methodology of this study as well as the key findings that revealed a huge gap in detecting web-based phishing threats and vulnerabilities with traditional security in place at these companies.

The objectives of Ermes' research were to measure how employees in a wide range of organization segments are exposed to contemporary cyberthreats. This includes providing insights on how companies and employees are routinely exposed to a variety of contemporary targeted web threats,[32] that are not ordinarily recognized or blocked by traditional company cyber ecosystems such as endpoint protection systems, firewalls and proxies (on premises and cloud).

A representative sample of 13 companies in several industries[33] were selected for this study conducted in 2020. A total of 361 employees were analyzed with an average of 28 employees per company.

Overall, a total of 86,754,580 connections were analyzed for potential cyber threats. Each of these companies had traditional security solutions[34] in place during the duration of the study which ranged from 8 to 31 days of monitoring employee Internet connections depending on the specific organization.

For each company Ermes conducted an audit by installing its proprietary software on the devices of each employee selected for the audit at the 13 companies. An average of 28 employees for each company had the software installed.

Throughout the duration of the study the software collected anonymous information about employees' navigation that is fully compliant with the General Data Protection Regulation (GDPR) of the EU and the EEA. This was done to ensure the preservation of all participants' privacy during the course of the research.

32. These contemporary targeted web threats include tracking of users and domains; session replay scripts; cryptomining; malicious clicks not blocked; and exposed titles, searches, and operating system data.

33. Industries for this research included food and beverage; aerospace; legal; luxury and fashion; consulting; manufacturing; public; and Retail.

34. Each company included in the Ermes' study was classified by the typology of the traditional security already in place: Endpoint protection, firewall, and proxy. All 13 organizations selected for this study had endpoint protection and firewalls in place. Only one company had EDR (extension) and 3 had cloud-proxy.

Copyright © 2021 Ermes Cyber Security S.R.L

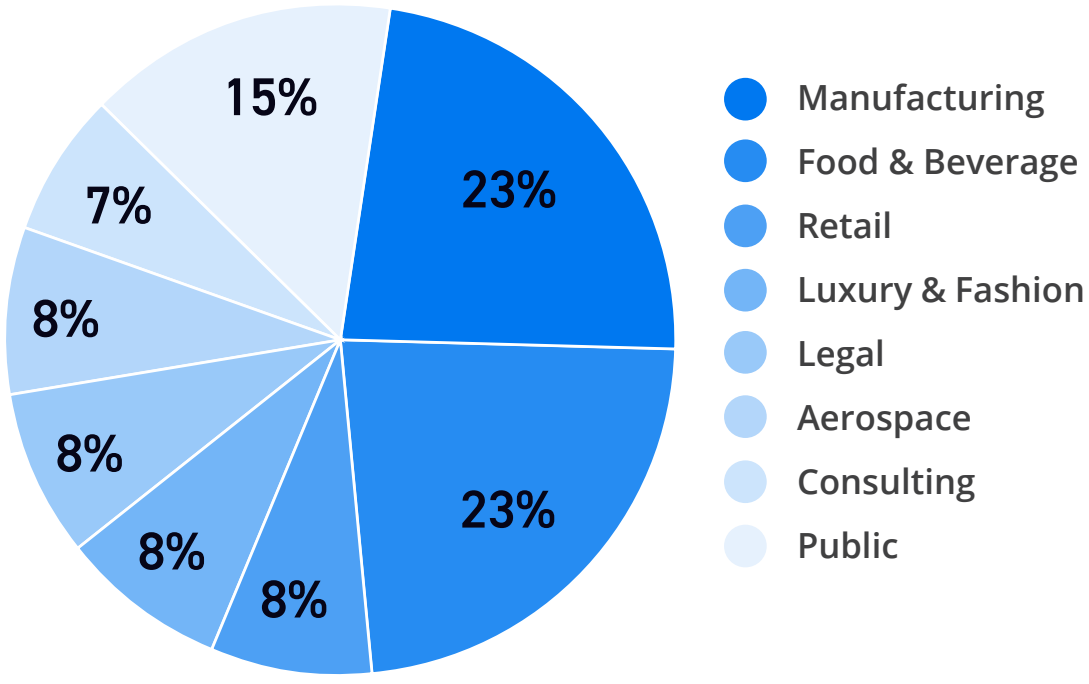
To monitor the potential threats to companies and employees, Ermes analyzed all of the 86,754,580 connections to specifically identify data exposures[35] that could have been subjected to a targeted cyberattack.

Of the analyzed connections that had been specifically identified as data exposures, Ermes checked to see how many were actually blocked by the traditional corporate security systems already in place at each of the organizations that participated in the study. Furthermore, Ermes then reviewed the actual web pages the employees visited and identified the malicious ones using its web classification services.

Ultimately, Ermes was able to determine exactly how many data exposures and malicious website visits were actually blocked by the traditional security apparatus in place at each of the 13 organizations.

Below are several graphs depicting information about the 13 organizations that participated in the Ermes study.

Industries of Companies in Study

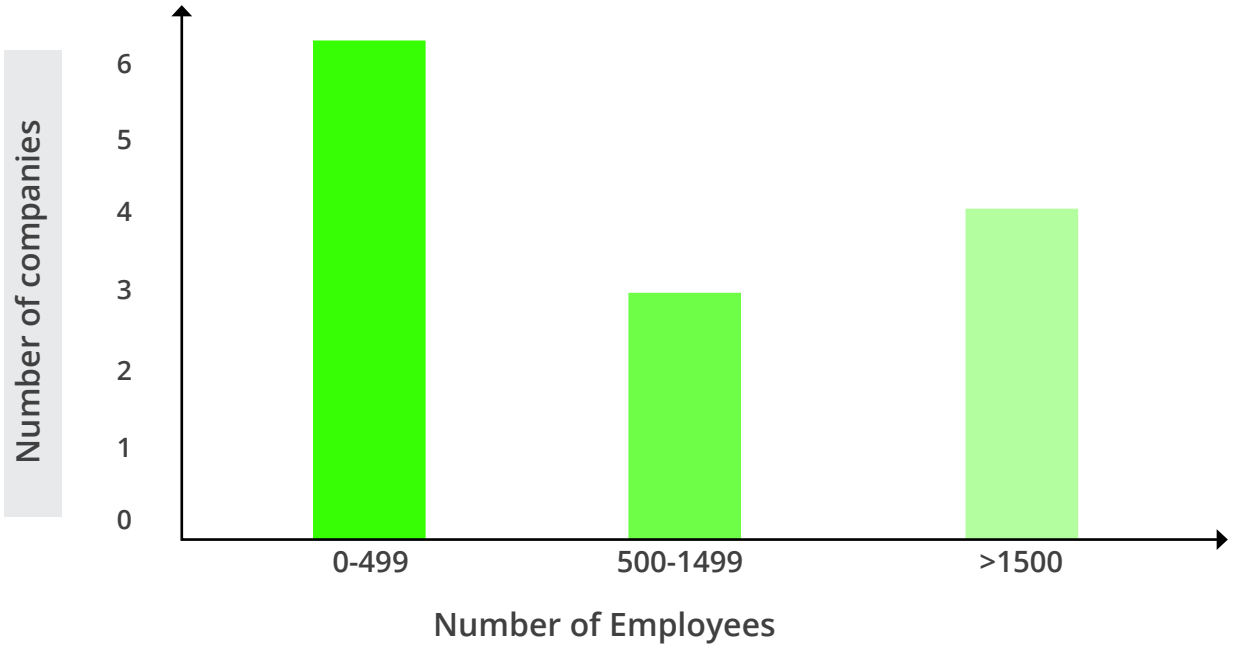


Source: Ermes Research 2020

35. For the purposes of this research, a data exposure was considered to be the disclosure of sensitive information that an attacker can use to capture the attention of an employee.

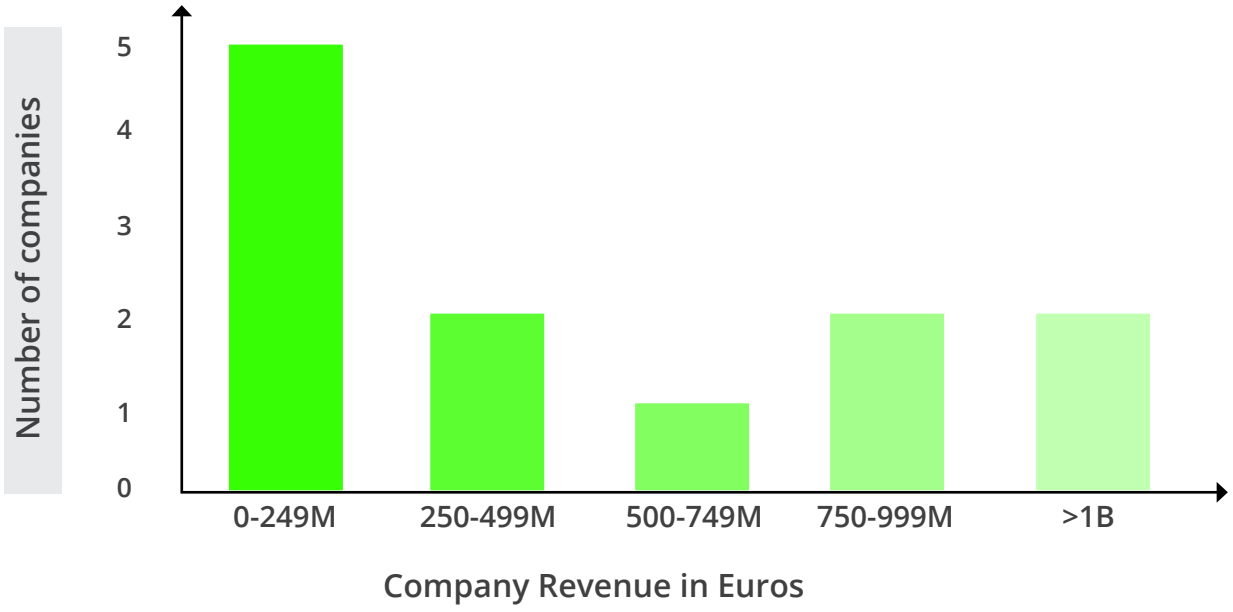
Copyright © 2021 Ermes Cyber Security S.R.L

Size of Companies in Study (By Number of Employees)



Source: Ermes Research 2020

Size of Companies in Study (by Revenues)

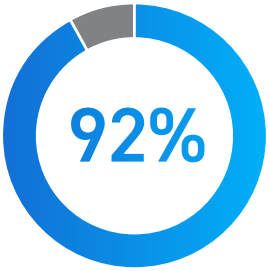


Source: Ermes Research 2020

One company did not report revenue because it is a public entity

Copyright © 2021 Ermes Cyber Security S.R.L

4 Employee Data Exposure



Overall, Ermes found that **91.97% of the employees participating** in the study had their data tracked by first- and third-party web tracking systems.

On average, **74.38%** of visited domains were also tracked. Moreover, Ermes' research discovered a significant amount of webpage title[36] and search query data being inadvertently exposed.

Browser information such as page titles and search queries can be used to retrieve user interests as well as preferences that an attacker can leverage to build a targeted attack. Moreover, the content of search queries is often quite private and personal: people are more likely to use search engines to look after issues they would not disclose to their closest friends.

140k
page titles exposed

33k
search queries exposed

A total of **139,783 titles were exposed** across the 13 companies with an average of 379-page titles exposed per employee. Likewise, a total of **33,026 search queries were exposed** with an average of 86 searches exposed per employee. Exposing title and search information increases the success of building a targeted attack by exposing highly detailed information. For example, the exposure of page titles and searches related to "mortgages" and "buying a house" is typical information that a cyber-criminal can specifically leverage in a phishing attack focused on a home buyer.

In addition to browser information, operating system data can be retrieved and maliciously exploited for vulnerabilities to plan a cyberattack. Through the use of extracted information from geolocation, battery status, language, and public IP addresses and ISP—cyber criminals can perfect the method and moment to deliver an attack.

36. The title tag is an HTML code tag that allows you to give a web page a title. This title can be found in the browser title bar, as well as in the search engine results pages (SERP).

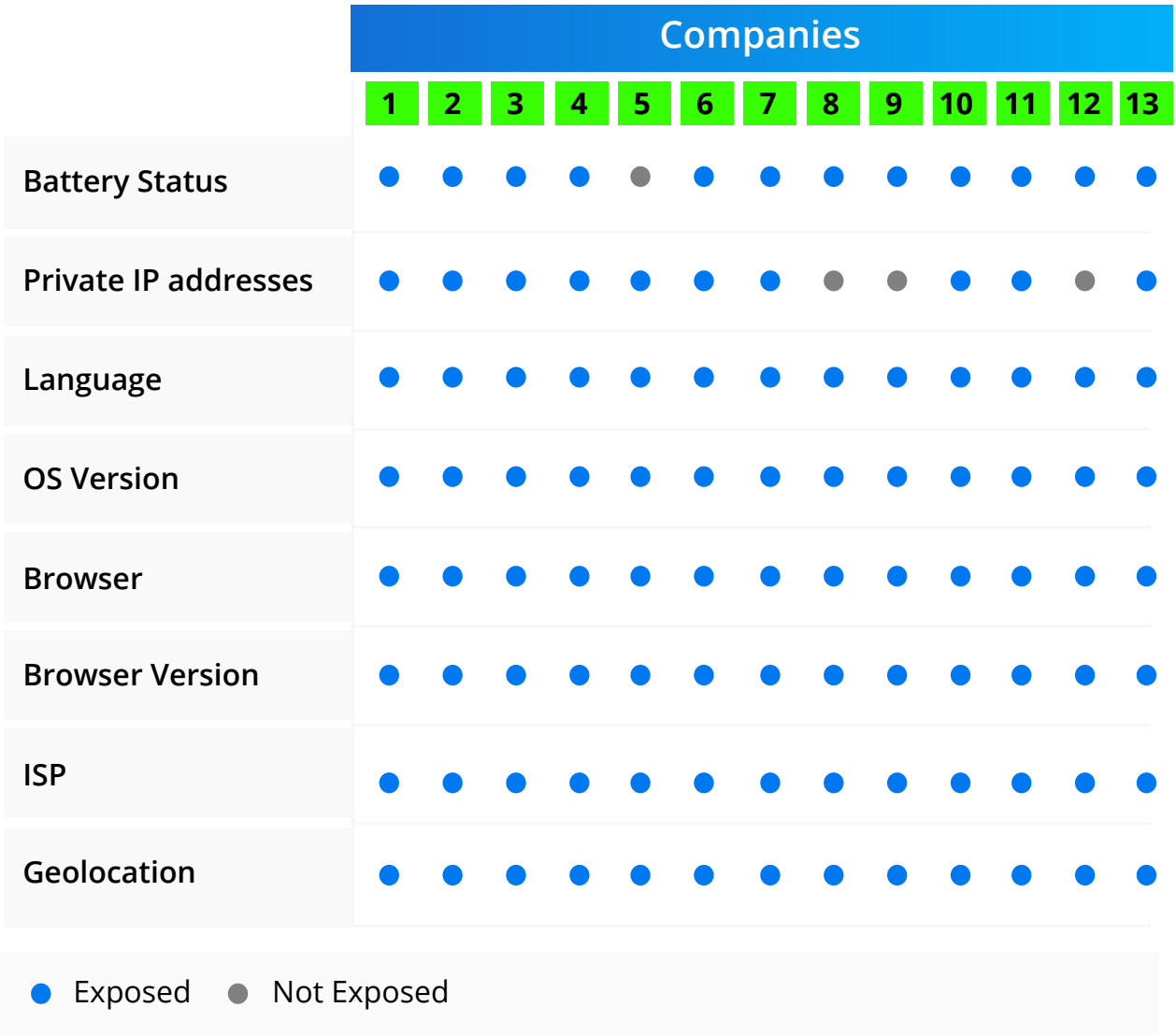
Copyright © 2021 Ermes Cyber Security S.R.L

The exposure of operating systems, browsers, and versions could lead to the disclosure of known software vulnerabilities that an attacker can ruthlessly exploit. For example, Windows 7 is not supported anymore and no longer receives security updates or fixes. Older browser versions such as these are extremely vulnerable to security issues that were corrected in subsequent versions.

Furthermore, through the use of exposed public IP addresses and ISP, information about geolocation and battery status can be exploited to determine when an employee is using a work device from home without entering the VPN that protects the company's cyber ecosystem. Typically, an attacker assumes a battery is discharging when a user is traveling and it is charging (or fully charged to 100%) when the employee is at home or work. Using battery data and geolocation, it is possible for an attacker to retrieve both work and home locations.

The heat map below visually depicts Ermes findings regarding the exposure of operating system information that can be used to plan an attack.

SYSTEM DATA EXPOSED BY COMPANY



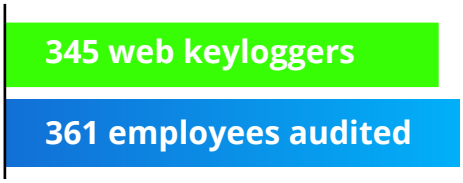
Copyright © 2021 Ermes Cyber Security S.R.L

5 Employee Risky Navigation and Browser Deterioration

Web keyloggers are a super-pervasive class of web trackers which record user actions on a web page. Clicks, scrolls, and data inserted on a form can be recorded and may include sensitive information such as credentials and credit card numbers.

Some of web keyloggers extract and register the whole webpage DOM, including all the information provided by visiting user. While not all of these recordings are malicious—some are done by legitimate services such as Hotjar and Yandex—the recording data can also be stolen by cyber criminals compromising company and employee information. These represent an actual increase of the company's vulnerability surface, with most of this area worryingly laying out of the control of administrator domain.

In the course of the Ermes' study, 345 web keyloggers were found to be contacted out of the 361 employees audited.



Web cryptomining typically makes unauthorized use of computing resources using simple third-party Javascript contained (legitimately or not) in web pages executed by the browser. They can severely deteriorate performance and device usability. During the audit performed in December 2020, 2 web cryptominers were detected at 1 company of the 13 that participated in the research. This was the only audit performed after the increase in Bitcoin value and PayPal's announcement that they would be accepting cryptocurrencies as payments on the platform.

This threat periodically gains momentum following cryptocurrency popularity trends. For instance, Monero (the main cryptocurrency used by web cryptominers) reached its maximum popularity when BitCoin was spiking in late 2017. We foresee a new increase of web cryptominer spread this year.

36. PayPal announced that it will enable cryptocurrency as a funding source for purchases in 2021, allowing users to use their cryptocurrency holdings to make purchases at its network of more than 26 million merchants. See PayPal at https://www.paypal.com/us/smarthelp/article/cryptocurrency-on-paypal-faq-faq4398.

Copyright © 2021 Ermes Cyber Security S.R.L

6 Malicious Websites

The two top attack methods mentioned above are the following:

Malware: the common name of a software developed by cyber-attackers that cause extensive damage to data and systems.

Phishing: A technique through which attackers take advantage of users' trust to convince them to reveal sensitive information. Spear phishing is a more sophisticated form that targets a specific individual or set of individuals.

As described in the previous sections, data collected by third party services might be used by harmful entities to lead users to malicious websites, such as phishing or malware delivery ones.

Ermes' research findings were that 93.2% of the navigations to malicious websites have not been prevented by the security solutions in place: indeed only 7 out of 104 attempts to reach malware or phishing websites were blocked.

From the data collected, Ermes was able to extrapolate that on average 4.38 malicious websites are visited by each employee every year: out of these 4.09 are not detected and prevented.

7 Conclusion

The key findings and insights learned from Ermes' research are the following:

- **91.97%** of employees in the study exposed data that might be used to build and deliver targeted cyberattacks.
- **4.38** malicious websites are visited on average by an employee every year.
- **4.09** malicious websites are visited on average by each employee every year and are not blocked by the traditional corporate security solutions in place.
- **93.2%** of the visits to malicious websites by employees were not blocked by traditional security solutions.

Copyright © 2021 Ermes Cyber Security S.R.L

From the research Ermes was able to conclude that an extremely high volume of personal information was shared by employees to the public. Such information could have been potentially exploited for malicious purposes and used to create custom cyberattacks. Leakage of these information extends the vulnerability surface of a company, with most of the sensitive data being in the hands of third-party companies, and so out of direct monitoring and control.

Even more critical, it was found that employees were attacked while navigating the web from work devices and that the existing security solutions in place were not able to effectively block these attacks.

Based on these findings, it is evident that relying exclusively on traditional corporate security solutions such as web/network filtering, and EDR do not provide enough protection against identifying and blocking malicious websites. In particular, two companies installing cloud-based proxy solutions from major vendors, were exposed and not protected. While these traditional solutions are very strong against “known” threats, there are many other threats that still remain undetected and invisible to these solutions.

To further fortify enterprises from being victimized by evolving and proliferating cybercrime, it makes sense to add the unique AI/deep-learning solution developed by Ermes to a corporate security portfolio which would have been able to prevent and detect all the threats described above.

For MSPs, systems integrators, distributors, and other third-parties that provide security services for their clients, the added-value of having a complementary solution—such as Ermes—in the portfolio is

1. To bolster security for client ecosystems through an additional layer of protection, and
2. Reduce the downtimes resulting from undetected threats and subsequent remedial interventions.

Copyright © 2021 Ermes Cyber Security S.R.L

> Cybercrime is the greatest threat to every company in the world

Ginni Rometty

Former Chairman, President, and CEO of IBM

Copyright © 2021 Ermes Cyber Security S.R.L

ABOUT

Through the use of artificial intelligence (AI) and deep-learning, Ermes–Intelligent Anti Phishing protects companies and employees from contemporary threats that users encounter while surfing the web. As a **leading innovator in web security and data protection,** we specialize in modern cyber threats that elude traditional security systems.

Our breakthrough technology provides visibility to undetected threats while effectively blocking modern, targeted web-based attacks on both PC and mobile devices, without the need to access the corporate virtual private network (VPN).

Through a **ground-breaking technology that combines prevention, protection and detection** Ermes has blocked 360+ billion connections and protected 30K+ people to date, providing unique and advanced solutions aimed at **disrupting cyber-attacks that continue to evade traditional security.**

CONTACT

Ermes Cyber Security S.R.L.
Corso Bernardino Telesio 29,
10146 Torino, Italy

info@ermes.company

www.ermes.company

Copyright © 2021 Ermes Cyber Security S.R.L