Turning Knowledge into Power

Trend Micro Research
Contents

Introduction: Knowledge is power ................................................................. 3
The malware evolution: How we got where we are today ............................ 4
The continuous search for knowledge ............................................................ 5
#1 Cyber threats ............................................................................................ 6
#2 Vulnerabilities and exploits ...................................................................... 7
#3 Targeted attacks and advanced persistent threats .................................. 9
#4 Artificial intelligence and machine learning .......................................... 11
#5 IoT, IIoT, OT ............................................................................................ 12
#6 The criminal underground ...................................................................... 13
#7 Future threat landscape .......................................................................... 14
Everyone benefits from Trend Micro Research ........................................... 15
Conclusion .................................................................................................... 16
INTRODUCTION

Knowledge is power

The volume and sophistication of new cyber threats is unrelenting, but there are ways to effectively deal with them and enable your business to be more secure. One critical way is through in-depth research that provides access to the methods and means of cybercriminals and expands the knowledge of how to better protect our world against cyberattacks.

To win against cyber threats, governments, universities, research institutions and private businesses must join together with the shared goals of understanding and anticipating the evolving threat environment, creating new cybersecurity technologies, and delivering innovation that continuously strengthens our digital protection.

Built into our security DNA, Trend Micro Research is at the forefront of understanding the global cybersecurity challenges facing our increasingly connected world. Our large, global team of dedicated experts enables us to provide our customers, public and private partners, and the broader digital community with in-depth information about threats—both current and emerging. Trend Micro Research is also instrumental in guiding the development of security tools to protect against these threats.

In this ebook, you’ll learn about the eight critical areas of cybersecurity and threat research on which Trend Micro Research focuses every day, in multiple locations around the world, and how this expert knowledge can be a powerful tool in protecting your organization, freeing you to focus on your business.

ANSWERING THE RIGHT QUESTIONS

What happened previously? What’s happening right now? What could happen in the future?

These fundamental questions drive all of our efforts at Trend Micro Research, which leads to insights and intelligence that ultimately help improve cybersecurity for everyone.
THE MALWARE EVOLUTION

How we got where we are today

Threat Landscape Evolution

The continuous search for knowledge

The only effective way to keep up with rapidly evolving threats and protect our digital assets, businesses, governments and critical infrastructure is through constant, comprehensive research.

Unlike the early days of malware when there were only a few variations to track, today’s cybersecurity research must cover a broad array of attack surfaces, methods and technologies. This includes analyzing the evolving tactics, techniques and procedures (TTPs) used by adversaries in sophisticated attacks such as advanced persistent threats (APTs). Researchers must also go “undercover” to where the bad actors are, anywhere in the world, to uncover new threats and trends.

Trend Micro Research covers all of these areas and more. It helps identify millions of threats daily and publishes innovative research on cybersecurity issues. As a leading provider of cybersecurity research and a partner to law enforcement, government, and other public entities, Trend Micro Research focuses on the critical components of today’s cybersecurity landscape:
#1: Cyber threats

Ongoing research and analysis of malware and threats provide a deeper understanding of how and why they work. This insight helps not only Trend Micro but also the broader cybersecurity community, businesses, and organizations improve prevention as well as threat detection and response.

For more than 32 years, Trend Micro Research has been analyzing malware and threats, turning its findings into actionable intelligence. Today the organization takes advantage of sophisticated tools for automation, machine learning and artificial intelligence (AI) to identify new threats more quickly and accurately than ever before. Experts then use re-engineering techniques to dissect the threats and understand how they are intended to work.

Our research coverage of malware and threats is both broad and deep, spanning across:

- Malware threats such as viruses, worms, Trojans, mobile malware, backdoors, remote access Trojans (RATs), fileless attacks, and others
- Web threats, including drive-bys, malvertisements, redirects, domain generation algorithms (DGAs) and command-and-control (C&C) servers
- Messaging threats such as spam, phishing, spear phishing, and business email compromise (BEC), as well as which internet protocol (IP) addresses are sending malicious emails

WHAT THIS MEANS FOR YOUR ORGANIZATION

54 BILLION THREATS were blocked by Trend Micro in 2019 thanks to intelligence generated by Trend Micro Research.

More than 46,000 command and control (C&C) servers were discovered and blocked by Trend Micro in 2019. Blocking cybercriminal infrastructure protects your organization from threats based on these sources, as well as exfiltration of stolen data.
#2: Vulnerabilities and exploits

Vulnerabilities are programming flaws that can be exploited by cybercriminals to bypass security and gain access to a system or network. An exploit is code that can be used to take advantage of a vulnerability. When a new vulnerability is discovered, it’s a race against time to patch it before exploits can be developed and deployed by bad actors.

Unfortunately, the number of vulnerabilities published every year continues to grow, with 21,273 published in 2019.¹ That’s why vulnerability research is essential in the fight against cyber threats. Vulnerability research identifies vulnerabilities in systems before they can be discovered and exploited for malicious purposes.

Trend Micro Research is the leader in vulnerability research, disclosing more than 52% of all publicly disclosed vulnerabilities in 2019 from 11 vendors in the study, according to analysis from Omdia. Through its Zero Day Initiative (ZDI) bug bounty program, Trend Micro is now a top reporter of Microsoft® and Adobe® vulnerabilities and a top reporter of vulnerabilities to ISC-CERT (part of the National Cybersecurity and Communications Integration Center focused on industrial control systems). Trend Micro Research identifies and discloses new vulnerabilities across a wide range of platforms, including:

- Operating systems (Windows®, Linux®, and Mac, among others)
- Applications (consumer and business)
- Mobile devices
- Industrial control systems and critical infrastructure

¹ “Common Vulnerabilities and Exposures List,” The MITRE Corporation.
Competing to find vulnerabilities in critical systems

The world’s largest vendor-agnostic bug bounty program, Trend Micro™ Zero Day Initiative (ZDI) was founded in 2005 to encourage coordinated disclosure of zero-day vulnerabilities to affected vendors by financially rewarding researchers through incentive programs. The ZDI program uses a Targeted Incentive Program and sponsored hacking contests to focus researchers’ attention on uncovering vulnerabilities in critical applications, operating systems, devices, and industrial control systems. The ZDI-sponsored Pwn2Own™ hacking contest challenges contestants to exploit widely used software and systems using previously unknown vulnerabilities. The contest demonstrates the vulnerability of devices and software in widespread use while providing a checkpoint on industry progress on fixing previously disclosed issues. Always focused on the evolving threat landscape, Pwn2Own Vancouver 2019 included a new automotive category, which resulted in the awarding of a Tesla Model 3. In January 2020, Pwn2Own Miami debuted with a focus on vulnerabilities in industrial control systems, and Pwn2Own 2020 in March was held fully virtual, reflecting the current global reality for travel while continuing the important work of discovering multiple new issues.
#3: Targeted attacks and advanced persistent threats

When threat actors want to breach a specific organization, they often use targeted attacks and advanced persistent threats (APTs). Whether they are after personal information, financial or payment data, medical information, credentials, intellectual property or some other target, cybercriminals often utilize an attack lifecycle that includes:

- Gathering open-source intelligence (OSINT) about their victims, from sources such as LinkedIn, Facebook and other social media
- Developing and deploying an initial attack vector
- Establishing command-and-control (C&C) connectivity
- Laterally moving across the victim’s network
- Identifying assets to steal
- Exfiltrating stolen data
- Initiating a maintenance stage to maintain persistence

Maintenance - attackers will do their best to maintain their foothold inside these stages.
#3: Targeted attacks and advanced persistent threats

CONTINUED

Analyzing the attack lifecycle helps security researchers understand how hackers evolve their TTPs and provides insight into how organizations can minimize the risk of being breached, as well as detect when a breach has occurred and remediate it.

Trend Micro researchers regularly analyze attacks against organizations, providing insight into each step of the attack life cycle and how best to protect against it. A recent example comes from Trend Micro's participation in the MITRE ATT&CK evaluation, which found MITRE taking on the persona of APT29, a threat group that has been attributed to the Russian government. This resulted in Trend Micro being ranked among the top tier of EDR vendors for our detection rates (91%, based on initial product configurations). Trend Micro also excelled at managing alert volumes to avoid alert fatigue as well as giving security analysts access to the type and depth of visibility they need when looking into detailed attacker activity—showing a great balance of detection capabilities (especially higher confidence detections) across the full attack chain. Our detection coverage results would have remained strong without human involvement—approximately 86% detection coverage. Our MDR service boosted it to 91%.

WHAT THIS MEANS FOR YOUR ORGANIZATION

Trend Micro gives you visibility into threats across your entire technology infrastructure to help identify attackers as they attempt to laterally move across a network. We do this by collecting threat intelligence from mobile, endpoint, server workloads (physical, virtual, cloud and containers), network, messaging, and gateway instances to correlate attack data.

Findings from Trend Micro Research contribute to the comprehensive defense and analytics capabilities of our products, which are used globally to identify targeted attacks and advanced threats. Trend Micro uses specialized engines, lateral movement detection, custom sandboxing, and seamless correlation across the entire attack lifecycle to detect threats.
#4: Artificial intelligence and machine learning

Artificial intelligence (AI) and machine learning (the method that helps AI-based systems get smarter) are critical capabilities for cybersecurity research and solutions, helping detect spam, phishing, exploits, and many other threats or attacks far faster and more accurately than humans.

Trend Micro researchers and data scientists have been working with these technologies since 2005, developing solutions to combat threats where AI and machine learning can be used to improve detection. Some of the many areas of use include detection of spam, phishing, malware, macro malware, exploits, malicious URLs and domains, social media threats, ransomware, business email compromise (BEC), targeted attacks, and domain generated algorithms (DGAs), as well as identification of good files.

Many forward-looking researchers are included in this group within Trend Micro Research. These researchers consider how AI and machine learning will be utilized to combat cyber threats in the future – as well as how cybercriminals may themselves use AI and machine learning to increase the frequency and success of attacks.

WHAT THIS MEANS FOR YOUR ORGANIZATION

More than 20 APPLICATIONS of AI and machine learning are already incorporated into Trend Micro products, giving you access to state-of-the-art security with advanced threat protection capabilities.

Recently MORE THAN 2,000 Trend Micro employees competed in an AI-focused development contest to improve their understanding of AI applications. This commitment and broad support across the company fosters further innovation using AI technology.
#5: IoT, IIoT, OT

Smart homes, smart factories, smart cars, and smart transportation systems are all part of the next wave of innovation that will transform how people and organizations use technology. However, cybercriminals and bad actors are also eager to exploit vulnerabilities in the devices, software, protocols, and apps used in the internet of things (IoT), industrial internet of things (IIoT), and operational technology (OT) that increasingly connects and controls our homes, businesses, factories and public infrastructure. Trend Micro researchers study these areas to better understand how these technologies are currently being used, how they could be used in the future, and how threat actors could potentially abuse them. Examples of our research areas include:

- Exploitation of vulnerabilities in robotic manufacturing and radio frequency (RF) equipment used in industrial machines
- Hacking of medical devices used in healthcare facilities
- Hijacking the communication protocols used by drones that have been approved for use over large groups of people
- Exploitation of consumer devices, such as kitchen appliances, smart TVs, and more, that are increasingly connected to the internet

WHAT THIS MEANS FOR YOUR ORGANIZATION

Trend Micro’s Smart Home Network solutions identified **MORE THAN 1.8 BILLION** malicious events on our customers’ home networks in 2019.

We launched Trend Forward Capital, a venture capital firm that is investing **US$100 MILLION** in support of unique IoT-focused companies.

We also recently launched a joint venture, **TXOne Networks**, focussed on helping Trend Micro be a leader in IoT security in the years to come.
Criminal underground communities can be a valuable source of information on everything from which cybercriminal groups are currently active to new TTPs used in the latest attacks. However, threat actors don’t work in an isolated area of the world; an actor in Russia may target an organization in the U.S. or South America. To have visibility into the entire threat landscape, researchers are needed within many regions throughout the world to collect and investigate threats and actor information.

Trend Micro employs researchers around the globe to analyze the many criminal undergrounds that exist, including those in Russia, China, North and South America, France, Germany, Japan, West Africa, and the Middle East.

Having regionally-supported researchers is critical, as many of these undergrounds operate based on local languages, norms and values, which researchers must understand in order to gain access to and participate in the community. This research gives Trend Micro valuable insight and threat intelligence that are used to protect customers from the threats employed by these bad actors.

Trend Micro operates 15 GLOBAL RESEARCH CENTERS for maximum coverage. We use the knowledge gained from research into criminal underground communities to improve our products and the protections used against the threats launched by these actors. This knowledge also helps to inform how we react to threats and helps our customers respond effectively to new attacks.

WHAT THIS MEANS FOR YOUR ORGANIZATION
#7: Future threat landscape

What will cyber threats be like in six months? Twelve months? Five years? How will malware continue to change and evolve? Which new forms of attacks will emerge?

Exploring and understanding all of these are the focus of forward-looking threat research: to anticipate the future threat landscape and which challenges enterprises, organizations and governments will face as they move to protect themselves and their customers, employees and constituents against new threats.

Trend Micro Research includes dedicated security experts who analyze the existing threat landscape and the overall computing landscape, including changes to infrastructure. They identify current and emerging trends, technologies, user behavior and market and geopolitical shifts that help them build predictive models of what the threat landscape will look like at intervals in the future.

The results of this research are published on a regular basis and available for business, technology and government leaders to use as a planning tool and guidance for cybersecurity strategies.

WHAT THIS MEANS FOR YOUR ORGANIZATION

Trend Micro’s history of innovation and hundreds of patents showcase our commitment to the development of technologies and solutions to protect our customers in the future. Our researchers work directly with the Trend Micro product development teams to build proof-of-concepts and ultimately embed or build new capabilities to protect our customers.
Everyone benefits from Trend Micro Research

It takes the collective efforts of many to thwart the malicious efforts of a few bad actors. By contributing analysis, insight and understanding across all seven critical areas explained in this ebook, Trend Micro Research helps improve cybersecurity for everyone.

Customers

**Product development:** Trend Micro Research provides product development teams with insights into how to protect against threats, which helps us improve protection capabilities and build new solutions for our customers. This process allows us to continually bring innovative new technologies and solutions to the market.

**Threat intelligence:** The Smart Protection Network is a global threat intelligence machine that collects, identifies, and helps protect Trend Micro customers from new threats. This 24/7/365 infrastructure is where many of the new protection capabilities are hosted once they are identified and published, delivering increased protection for our consumer, business and government customers around the world.

Public and private partnerships

Trend Micro is active in public and private partnerships that focus on helping organizations around the world improve cybersecurity. For example, we work extensively with law enforcement organizations such as the U.S. Federal Bureau of Investigation and the U.S. Secret Service. We also have a researcher on staff at Interpol Cyber Headquarters in Singapore to help with investigations aimed at bringing cybercriminals to justice. Part of this interaction includes working with organizations that can help dismantle criminal infrastructures, including botnets.

We are partners with Information Sharing and Analysis Centers (ISACS) and the Consortium for Electric Reliability Technology Solutions (CERTS) for the infrastructure industry, as well as the Health Information Trust Alliance (HITRUST), which focuses on information security for the healthcare industry. We partner with several major healthcare providers in the U.S. to improve the sharing process for threat intelligence.

Technology vendors

We help vendors of operating systems and applications such as Adobe, Microsoft, and VMware® create patches against vulnerabilities ahead of public disclosure. We’re also committed to long-standing relationships with leading software vendors and the research community to influence the importance of security in the product development life cycle.

IoT/IoT manufacturers

Trend Micro helps IoT and IIoT manufacturers improve the security of their products and the wider IoT/IoT ecosystem, enhancing protection throughout the entire device lifecycle. In fact, Trend Micro and Moxa, a leader in OT technology, recently launched a joint-venture called TXOne Networks to focus on securing industrial systems.
Conclusion

Committed to securing our increasingly connected world, Trend Micro invests heavily in security research capabilities as well as the people who perform these functions, recognizing that threat actors never stop and are constantly changing how they attack people and organizations around the globe. This investment allows us to turn knowledge into power, providing critical information for use in our products as well as fueling innovation in new technologies to protect against threats today and those that will come in the future.

Stay up-to-date on the latest threats and the shifts in cybercriminal activities by following our blogs, research reports, and security reports within our Research section on our website.

About Trend Micro Research

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information. Our innovative solutions provide our customers with layered security for data centers, cloud workloads, networks, and endpoints.

At the heart of our leadership, Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights with the public, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on targeted attacks, artificial intelligence, Internet of Things (IoT), cybercriminals, and more. We continually work to anticipate the next wave of threats and deliver thought-provoking research that can shape strategic industry direction.

For more information, visit www.trendmicro.com