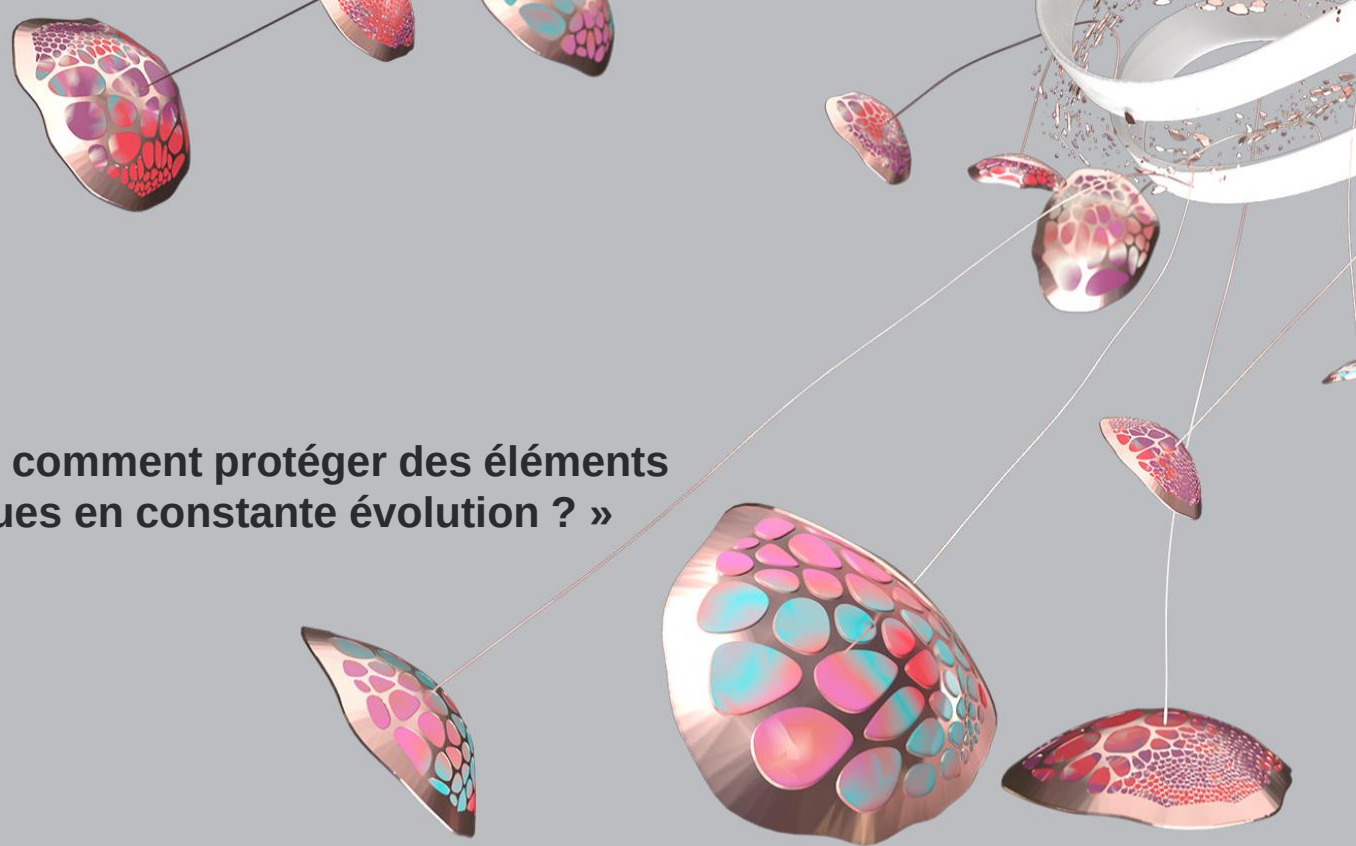


" Etablissements de santé : comment protéger des éléments disparates face à des attaques en constante évolution ? »

Nicolas ARPAGIAN,
Director Cyberscurity Strategy

22 septembre 2022

@cyberguerre

Nicolas ARPAGIAN

@cyberguerre

- Director, Cybersecurity Strategy

TREND MICRO™

- Enseignant

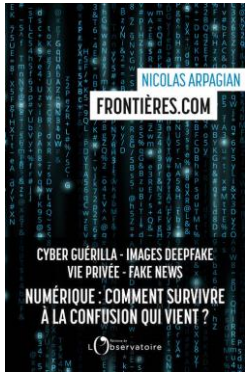
ENSP ÉCOLE NATIONALE SUPÉRIEURE DE LA POLICE

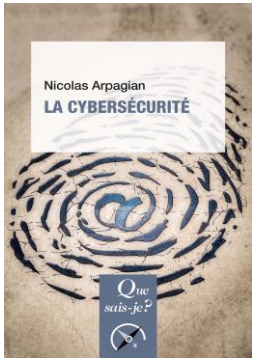
ENM ÉCOLE NATIONALE de la MAGISTRATURE

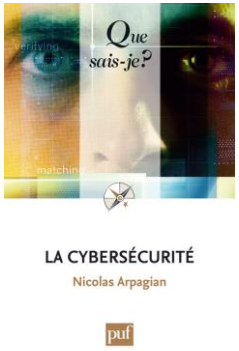
Sciences Po Saint-Germain en-Laye

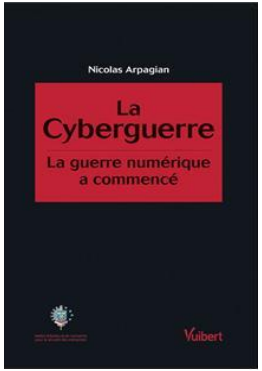
EGE Ecole de Guerre Economique

- Auteur









Des coopérations à l'échelle internationale

Spécialiste de l'analyse de la cybermenace **depuis plus de 30 ans** (1989).

Environ 2Md$ de chiffre d'affaires en 2021.

Une entreprise bénéficiaire depuis sa cotation en Bourse en 1998.

+500 000 entreprises clientes, incluant 9 des 10 premières sociétés du Global Fortune 500.

7 000 collaborateurs présents dans 65 pays.

TREND MICRO A LEADER IN MAJOR ANALYST EVALUATION CATEGORIES

The results are in from 2021 vendor evaluations and it's great news for Trend Micro's cybersecurity platform. We've been named a Leader in each of the major evaluation categories from top analyst and third-party firms; MITRE, Forrester, IDC, and Gartner.

Trend Micro is the ONLY cybersecurity vendor to achieve this feat.

In our view, it's yet more confirmation that Trend Micro continues to be the cybersecurity provider analysts trusted most during the uncharted issues brought on by the COVID-19 pandemic, including the sudden shift to a remote workforce and the vulnerabilities exposed by this migration.

See all new analyst reports

Gartner

Named a Leader, 2021 Gartner™ Magic Quadrant for Endpoint Protection Platforms (EPP)

FORRESTER®

Named a Leader, Extended Detection and Response (XDR) Providers, Q4 2021

FORRESTER®

Named a Leader, Enterprise Email Security, Q2 2021

MITRE

Top 3 for Visibility and Telemetry, Q2 2021

FORRESTER®

Named a Leader, Endpoint Security SaaS, Q2 2021

IDC
Analyze the Future

#1 Total Market Share, Worldwide Corporate Endpoint Security 2020

Gartner

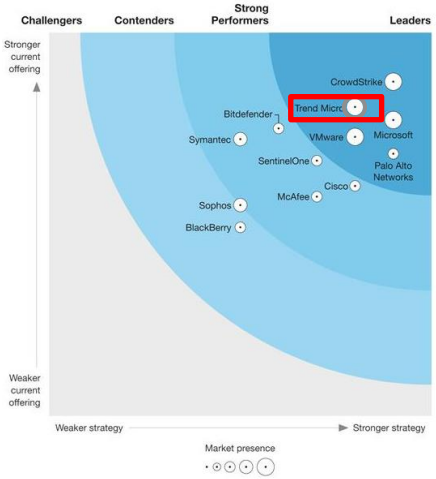
A Customers' Choice in the October 2021 Gartner Peer Insights™ 'Voice of the Customer': Endpoint Protection Platforms

TREND MICRO™

Protéger les différents environnements techniques

Endpoint Security Software as a Service

Q2, 2021

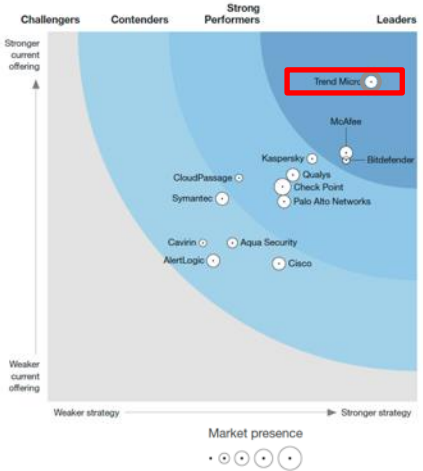


Enterprise Email Security

Q2, 2021

Cloud Workload Security

Q4, 2019



Enterprise Detection and Response

Q1, 2020

Threat landscape

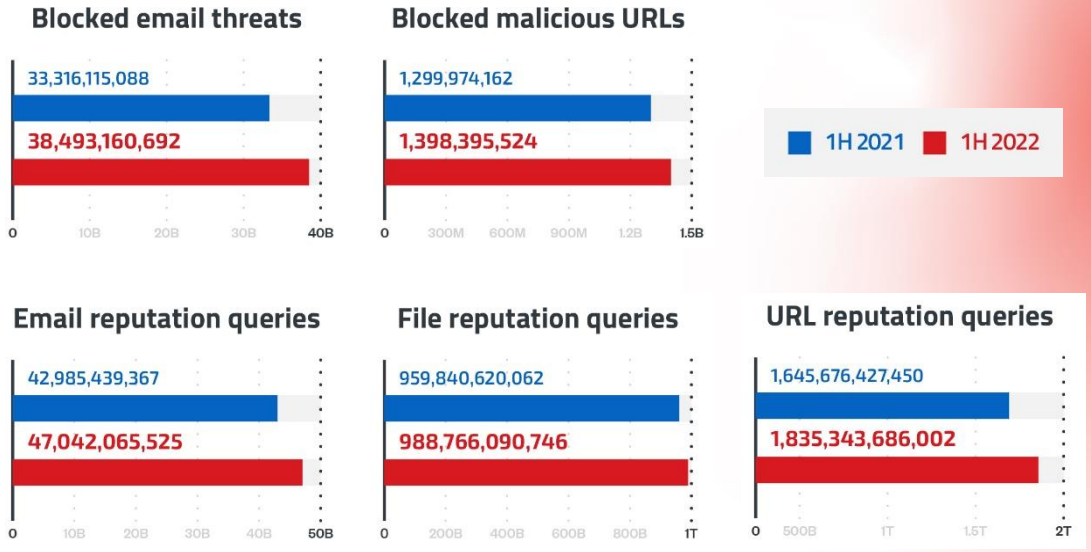
In the first half of 2022, the Trend Micro Smart Protection Network protected users from more than 63 billion threats consisting of email threats, malicious files, and malicious URLs.

63,789,373,773

Overall number of threats blocked for the first half of 2022

2,911,929,067,913

Overall queries

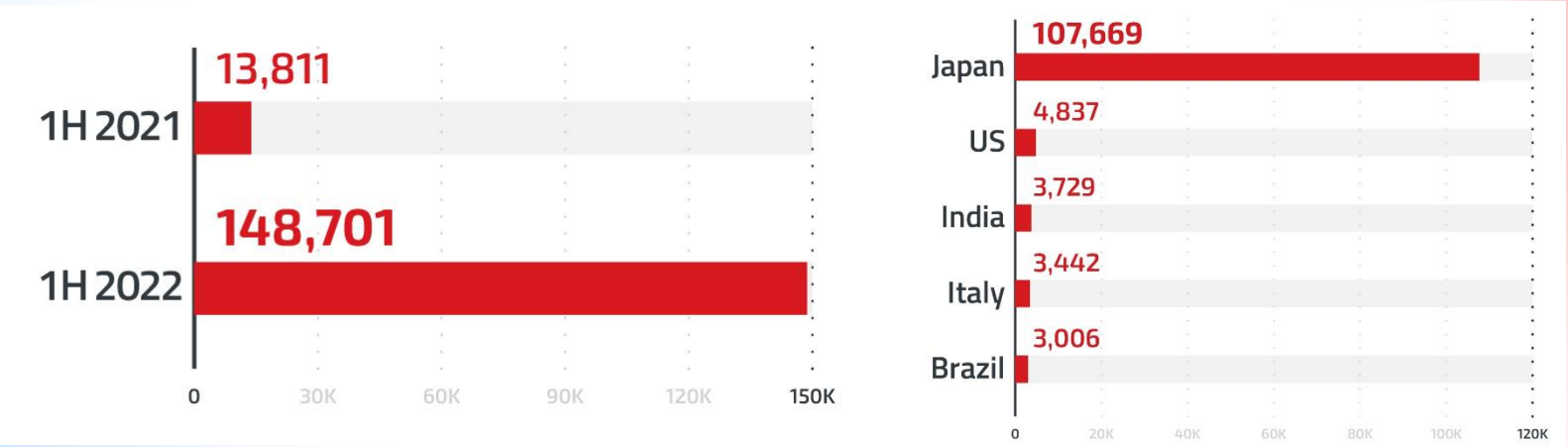


Source: Trend Micro Smart Protection Network (SPN)

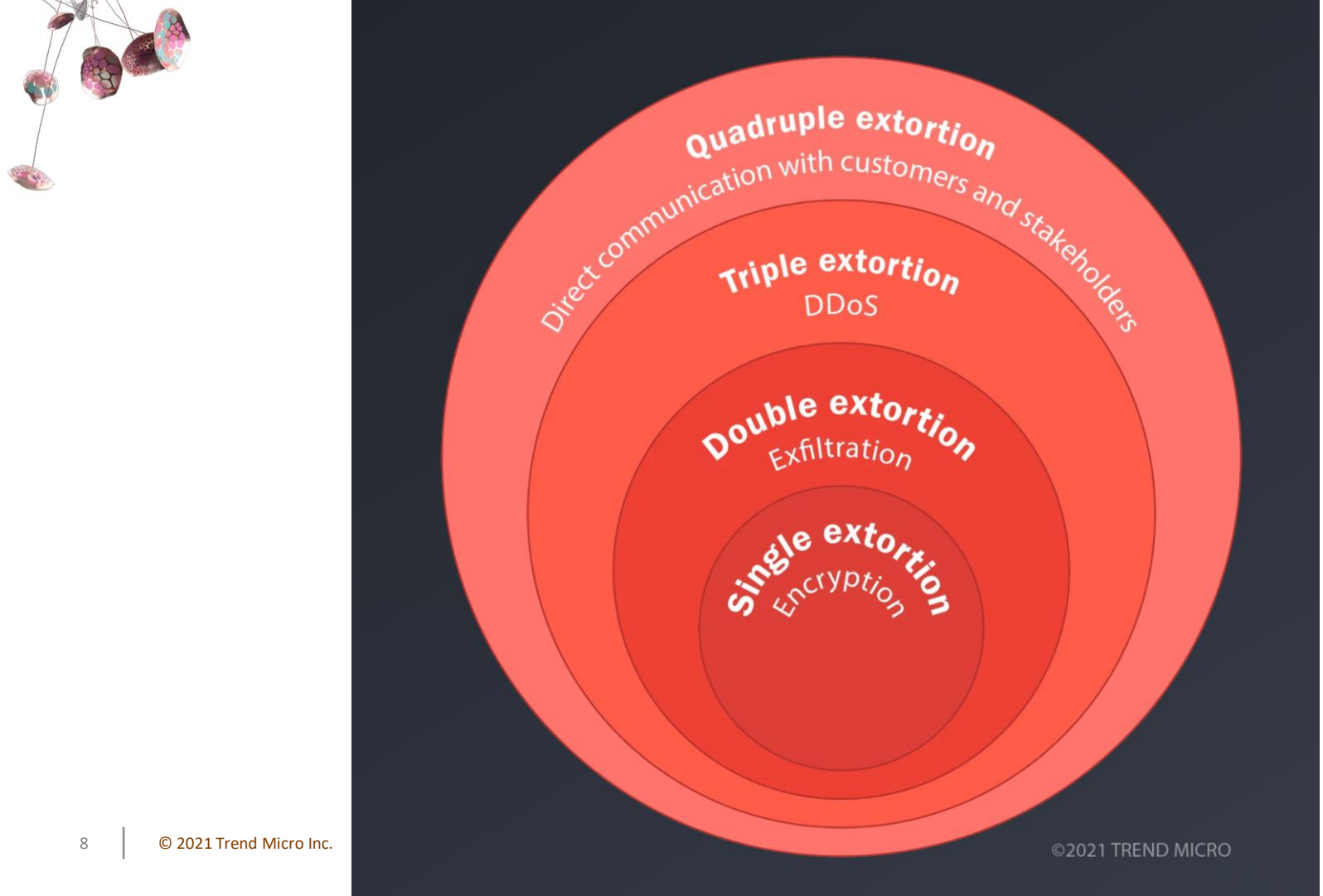
Ransomware

Despite the dismantling of the Emotet botnet's infrastructure in 2021, it remains a popular malware choice in the malware-as-a-service (MaaS) industry. The Conti ransomware operators were found using Emotet as a loader, and early this year, new Emotet variants surfaced.

We saw a whopping 976.7% increase in Emotet detections in the first half of 2022 compared to the first half of 2021, with Japan having the highest number of detections.

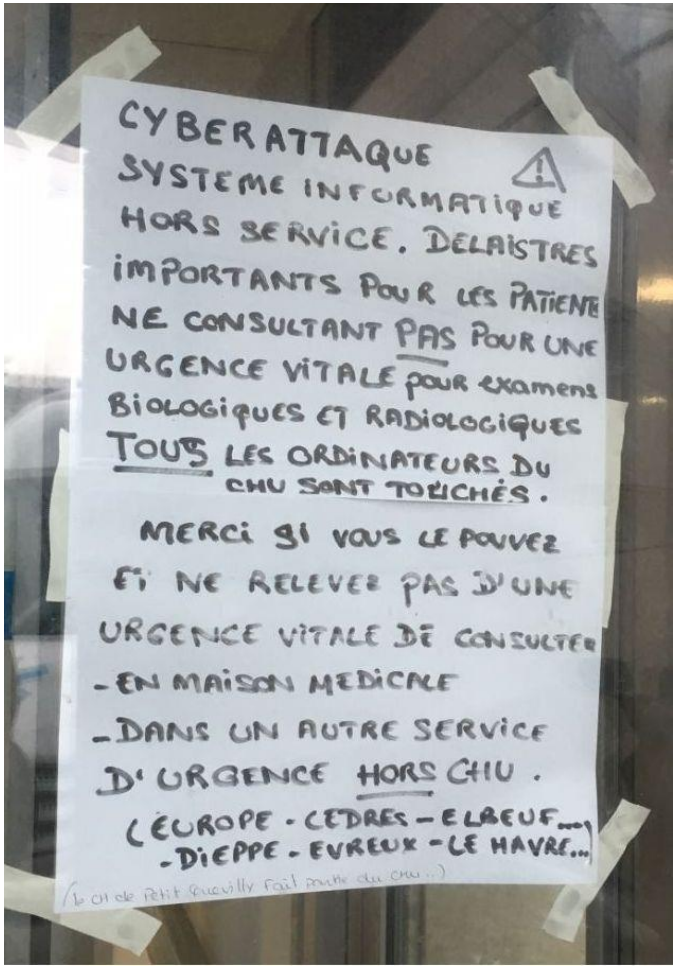


Source: Trend Micro Smart Protection Network (SPN)



16 novembre 2019 - CHU de Rouen

Attaque par rançongiciel :
chiffrement des informations essentielles permettant la gestion des blocs opératoires, des pharmacies, des prescriptions et des admissions.



L'hôpital de Dax en partie paralysé par une attaque informatique

Un logiciel malveillant a bloqué, mardi, le fonctionnement du système informatique de l'hôpital landais, le rendant inaccessible. Le centre de vaccination contre le Covid-19 a dû fermer ses portes.

Par Claire Mayer (Bordeaux, correspondante)

Publié le 10 février 2021 à 10h15 - Mis à jour le 11 février 2021 à 06h01 • Lecture 3 min.

Cyberattaque à Angers : la ville du futur au défi d'un piratage massif

Une cyberattaque a paralysé les ordinateurs et les services en ligne de la ville d'Angers qui aspire à devenir la métropole la plus connectée du pays dans les prochains années.

Cyberattaque confirmée au centre hospitalier de Villefranche-sur-Saône

L'établissement de santé a signalé un important incident, affectant son informatique, sa messagerie et sa téléphonie. Plusieurs services normalement exposés sur Internet apparaissent actuellement injoignables.

INDEPENDENT

Cyberattaque: le personnel du NHS n'a pas pu accéder aux notes des patients pendant trois semaines

La cyberattaque a ciblé les systèmes du NHS utilisés pour envoyer des ambulances et pourrait durer des semaines, a déclaré le personnel du NHS

Rebecca Thomas Correspondant santé • Mercredi 10 août 2022 18:20 • 28 Commentaires

US govt warns of Maui ransomware attacks against healthcare orgs

By **Sergiu Gatlan**

July 6, 2022 10:47 AM 0

TREND MICRO

Tech & web

Actualités tech | Crypto | Start-up | Tests | Pratique | Jeux vidéos

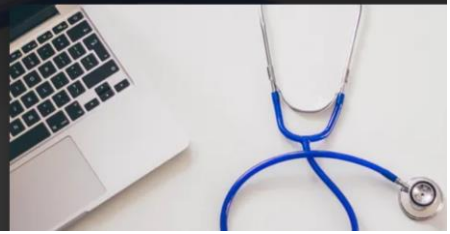
Pourquoi les hôpitaux français sont des proies faciles pour les cybercriminels

Par **Elsa Bembaron**
Publié le 24/08/2022 à 20:15, mis à jour le 25/08/2022 à 11:06

france culture | Grille des programmes | Podcasts | Fictions | Documentaires | Savoirs | Arts et Création

Protection des données de santé : encore trop de failles

Mardi 14 septembre 2021



Les équipements médicaux obsolètes, une menace majeure

Chweta Sharma, CSO (traduit et adapté par Jacques Cheminat), publié le 02 Février 2022

Selon une étude, les équipements IoT de santé fonctionnant avec des versions obsolètes de Windows ou Linux sont des cibles faciles, notamment pour les gangs de ransomware. La segmentation réseau peut-être une solution à condition de respecter un certain équilibre.

LEMONDE INFORMATIQUE

75% des prestataires de santé utilisent des équipements au système d'exploitation obsolète

Developpez.com

En France, seuls 10% d'entre eux assurent que leurs équipements utilisent les dernières versions logicielles

Le 27 janvier 2022 à 21:26, par Sandra Coret | **5 commentaires**

TREND MICRO

Microsoft | Support technique Microsoft 365 Plus Achetez Microsoft 365 Tout Microsoft

Produits Appareils Nouveautés Compte et facturation Modèles Prise en charge accrue

Le support de Windows XP a pris fin

Windows XP, Windows 10

Que signifie la fin du support de Windows XP ?

Microsoft a assuré le support de Windows XP pendant les 12 dernières années. Il est temps désormais, pour nous et nos partenaires fabricants de matériel et de logiciels, d'investir nos ressources dans le support de technologies plus récentes afin de pouvoir continuer à vous offrir de nouvelles expériences inoubliables. Par conséquent, l'assistance technique pour Windows XP n'est plus disponible, y compris les mises à jour automatiques permettant de protéger votre PC.

Microsoft a également mis fin à la possibilité de télécharger Microsoft Security Essentials sur Windows XP. Si vous avez déjà installé Microsoft Security Essentials, vous continuerez à recevoir les mises à jour des signatures anti-programmes malveillants pendant une durée limitée. Toutefois, notez que Microsoft Security Essentials (ou tout autre logiciel antivirus) aura une efficacité limitée sur les PC ne disposant pas des dernières mises à jour de sécurité. Cela signifie que les PC exécutant Windows XP ne seront pas sécurisés et seront vulnérables aux infections.

Microsoft | Support Microsoft 365 Office Windows More All Microsoft

Windows support Products Devices What's new Get Windows 11 More support

Windows 7 support ended on January 14, 2020

Windows 7

Microsoft made a commitment to provide 10 years of product support for Windows 7 when it was released on October 22, 2009. This 10-year period has now ended, and Microsoft has discontinued Windows 7 support so that we can focus our investment on supporting newer technologies and great new experiences. The specific end of support day for Windows 7 was January 14, 2020. Technical assistance and software updates from Windows Update that help protect your PC are no longer available for the product. Microsoft strongly recommends that you move to Windows 11 to avoid a situation where you need service or support that is no longer available.

Windows 10 Home and Pro

Windows 10 Home and Pro follows the Modern Lifecycle Policy.

This applies to the following editions: Home, Pro, Pro Education, Pro for Workstations

Important

Beginning with Windows 10, version 21H2 (the Windows 10 November 2021 Update), feature updates will be released annually in the second half of the year via the General Availability Channel. Go **here** to learn more. Microsoft will continue to support at least one Windows 10 release until October 14, 2025.

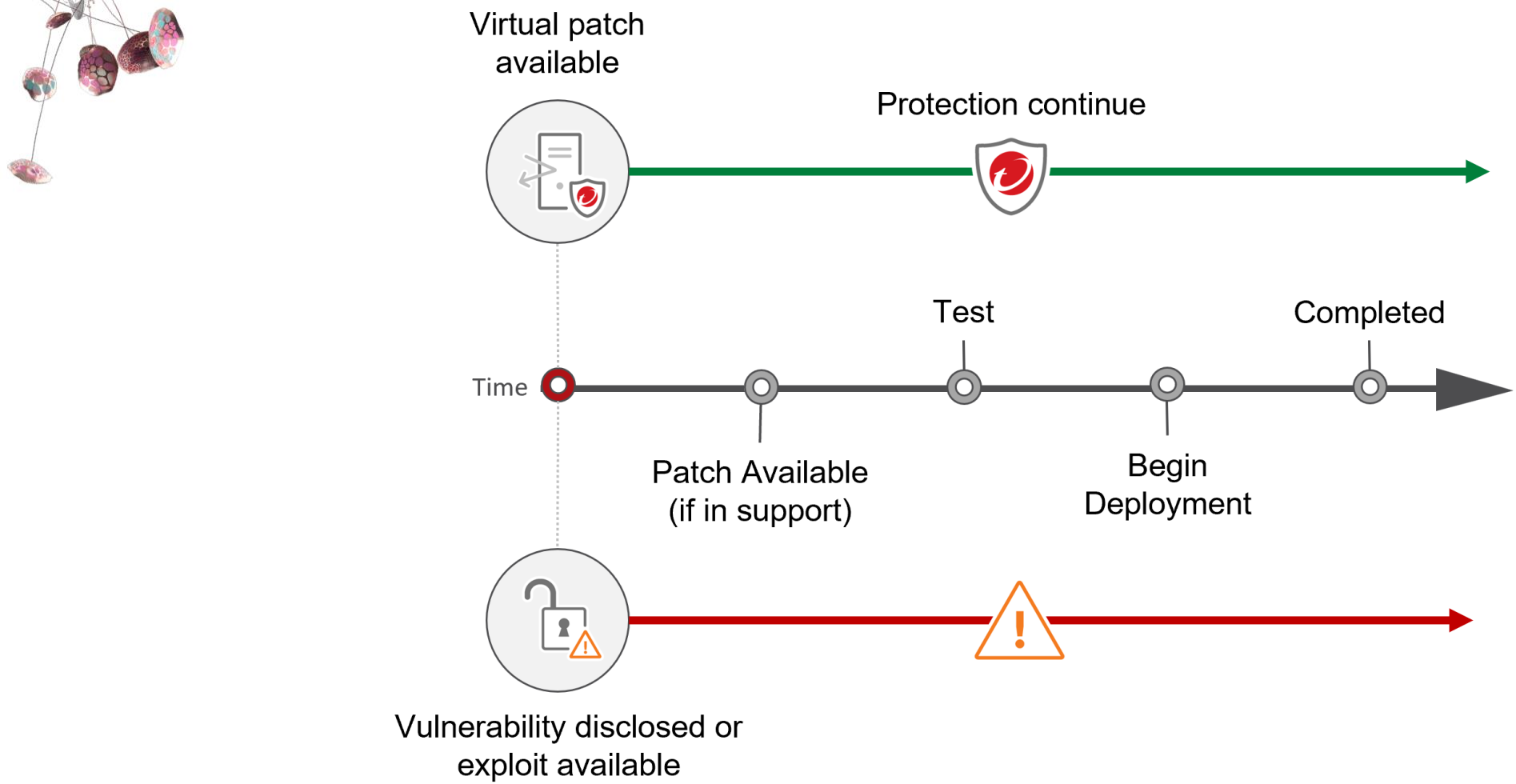
Support dates are shown in the Pacific Time Zone (PT) - Redmond, WA, USA.

Support Dates

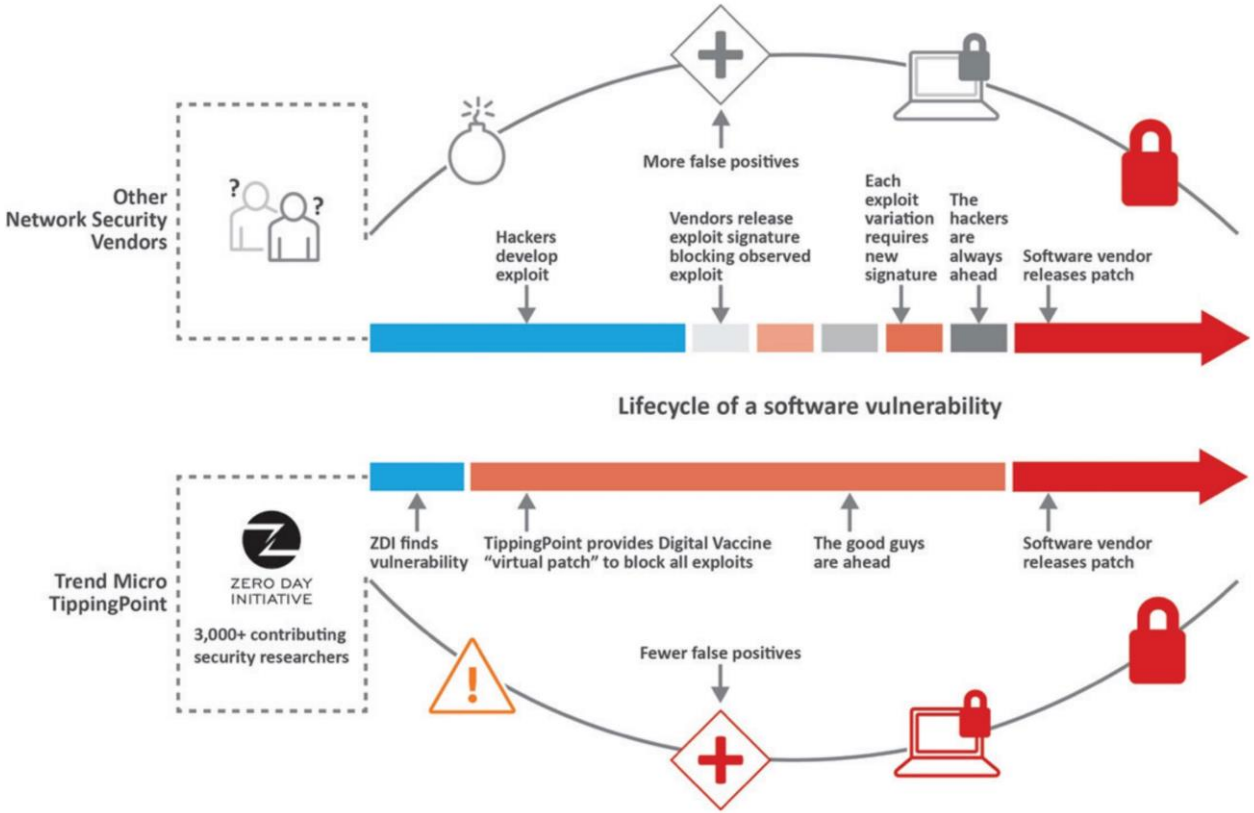
Listing	Start Date	Retirement Date
Windows 10 Home and Pro	Jul 29, 2015	Oct 14, 2025

The following table lists the End of Service (EOS) dates for each version of [redacted] Critical System Protection.

Sr. No.	Product	Version	GA	EOS*
1	[redacted] Critical System Protection	8.0.2	23-Dec-21	23-Dec-23
2	[redacted] Critical System Protection	8.0 MP1 HF2	15-Mar-20	16-Jun-22
3	[redacted] Critical System Protection	8.0 MP1 HF1	15-Nov-19	31-Mar-21
4	[redacted] Critical System Protection	8.0 MP1	20-May-19	31-Mar-21
5	[redacted] Critical System Protection	8.0.0	1-Oct-18	31-Mar-21
6	[redacted] Critical System Protection	7.2 MP2	5-Oct-18	31-Mar-21
7	[redacted] Critical System Protection	7.2.0	2-Oct-17	31-Mar-21
8	[redacted] Critical System Protection	7.1.0	5-Jun-17	31-Mar-21
9	[redacted] Critical System Protection	7.0.0 MP2	30-May-17	31-Mar-21
10	[redacted] Critical System Protection	6.5.1 MP2	2-Jun-17	31-Mar-21



SOFTWARE VULNERABILITY LIFECYCLE



Through our ZDI program, Trend Micro customers have an average of **96 days** of preemptive protection against vulnerabilities ahead of vendor patches.

TREND MICRO ZERO DAY INITIATIVE

https://www.zerodayinitiative.com/

The Zero Day Initiative (ZDI) was created to encourage the reporting of 0-day vulnerabilities privately to the affected vendors by financially rewarding researchers. At the time, there was a perception by some in the information security industry that those who find vulnerabilities are malicious hackers looking to do harm. Some still feel that way. While skilled, malicious attackers do exist, they remain a small minority of the total number of people who actually discover new flaws in software.

Incorporating the global community of independent researchers also augments our internal research organizations with the additional zero-day research and exploit intelligence. This approach coalesced with the formation of the ZDI, launched on July 25, 2005. The main goals of the ZDI are to:

Amplify the effectiveness of our team by creating a virtual community of skilled researchers.

Encourage the responsible reporting of zero-day vulnerabilities through financial incentives.

Protect Trend Micro customers from harm until the affected vendor is able to deploy a patch.

Today, the ZDI represents the world's largest vendor-agnostic bug bounty program. Our approach to the acquisition of vulnerability information is different than other programs. No technical details concerning the vulnerability are sent out publicly until the vendor has released a patch.

We do not resell or redistribute the vulnerabilities that are acquired through the ZDI.

Avril 2022

Lors du Pwn2Own Miami, 26 failles zero day sur des ICS et Scada découvertes

Tesla, Microsoft and Ubuntu bugs found during Pwn2Own hacking competition

Several bugs in Microsoft, Ubuntu and Tesla products were found and exploited during the three-day Pwn2Own hacking conference in Vancouver this week.

The conference – organized by Trend Micro's Zero Day Initiative – gives hackers a chance to earn money in exchange for discovering and exploiting vulnerabilities in popular products.

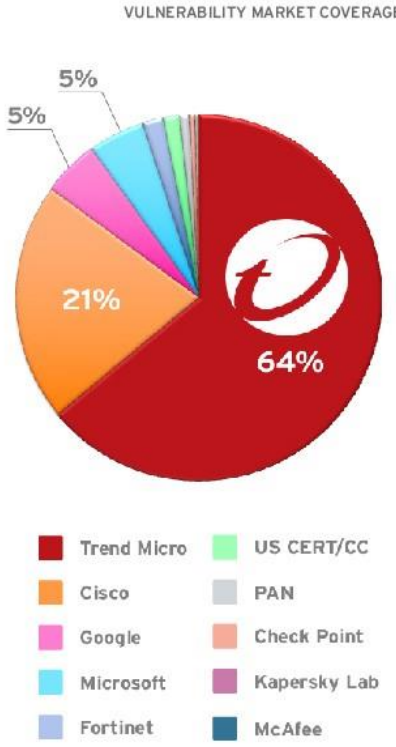
By the end of day two on Thursday, the conference had paid out $945,000 in rewards, including $75,000 to hackers with offensive security company Synacktiv for two unique bugs found in the Tesla Model 3 Infotainment System.

Mai 2022

TREND MICRO™ ZERO DAY INITIATIVE™

Leader in Global Vulnerability Research and Discovery Since 2007

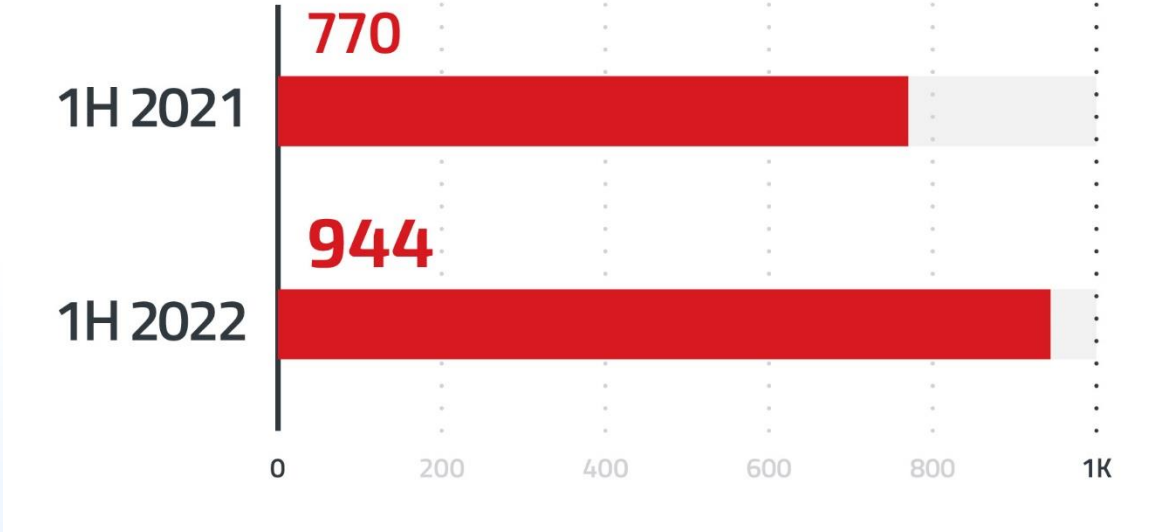
TREND MICRO



TREND MICRO

Vulnerabilities

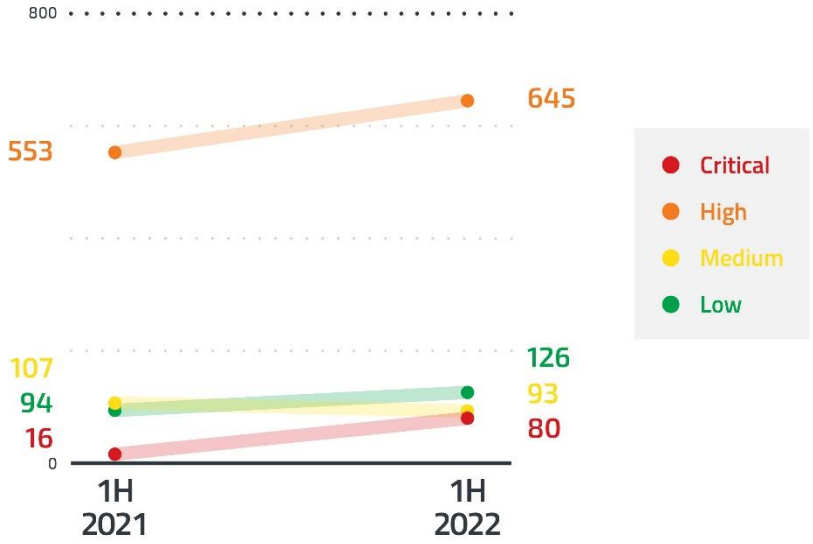
The Trend Micro™ Zero Day Initiative™ (ZDI) published advisories on 944 vulnerabilities, which is approximately 23% higher compared to the number of disclosed vulnerabilities in the first six months of 2021.



Source: Trend Micro™ Zero Day Initiative™

Vulnerabilities

Vulnerabilities with a high-severity rating made up the greatest portion (68%) of the published vulnerabilities. In the first half of 2022, critical- and high-severity vulnerabilities also saw large increases.



Source: Trend Micro ZDI program

August 2022 - Announcing new disclosure timelines for bugs resulting from incomplete patches.

Malware Scanning and Cleanup Tool for Air-gapped Systems and Standalone PCs

Supported OS

Windows	Windows Embedded	Linux
Windows 2000 SP3 / SP4 *3 Windows XP Professional SP1 / SP2 / SP3 *4 Windows Vista SP1 / SP2 Windows 7 SP1 Windows 8 *2 Windows 8.1 *2 Windows 10 Windows 11 Windows Server 2003 R2 Windows Server 2008 SP2 Windows Server 2008 R2 SP1 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019	Windows XP Embedded SP1 / SP2 / SP3 *5 Windows Embedded Standard 2009 *5 Windows Embedded Standard 7 Windows Embedded POSReady 2009 Windows Embedded POSReady 7 Windows XP Professional for Embedded Systems Windows Vista for Embedded Systems SP1 / SP2 Windows 7 for Embedded Systems SP1 Windows 8 Standard for Embedded Systems Windows 8.1 Pro / Industry for Embedded Systems Windows 10 IoT Enterprise Windows 11 IoT Enterprise Windows Server 2003 for Embedded Systems SP1 / SP2, R2 Windows Server 2008 for Embedded Systems, R2 Windows Server 2012 for Embedded Systems, R2	CentOS 6 CentOS 7 CentOS 8 Red Hat Enterprise Linux 6 Red Hat Enterprise Linux 7 Red Hat Enterprise Linux 8 Ubuntu Linux 14.04 to 20.10

Trend Micro Warns of 75% Surge in Ransomware Attacks on Linux as Systems Adoptions Soared

63 billion threats blocked by Trend Micro in 1H 2022

TREND MICRO™

Merci !