Blog

Discover our cybersecurity articles

underground card shop banner

Credit Card Fraud Investigation: State of Underground Card Shops in 2022

20.May.2022

Beatriz Pimenta Klein and Lidia López Sanz, Threat Intelligence Analysts

In our latest credit card fraud investigation blog our threat intelligence analysts investigate the current card shop ecosystem, from active shops and the return of Rescator as well as other recently shuttered card shops and credit card fraud to look out for.

Read More

The State of Ransomware in 2022

The State of Ransomware in 2022

17.May.2022

Blueliv, an Outpost24 company

Ransomware continues to be a prevalent threat to almost every modern industry after a sudden renaissance at the beginning of the COVID-19 pandemic as threat actors sought to capitalize on overwhelmed organizations and their suddenly vulnerable employees.

Read More

FTSE 100 credential theft study

FTSE 100 credential theft study 2022

10.May.2022

Corporate credential theft is a targeted effort and makes FTSE 100 companies credentials particularly attractive to cybercriminals with accelerated digital transformation (BYOD and hybrid working). Once an attacker gets hold of stolen user credentials and passwords, they can sell the credentials in the cybercrime underground or use them to compromise an organization’s network, bypassing security measures and threaten the credibility and integrity of the institution.

Read More

The most critical vulnerabilities right now - April 2022

The most critical vulnerabilities right now - April 2022

02.May.2022

Blueliv, an Outpost24 company

The first few months of 2022 have brought with them plenty of breaches and vulnerabilities for threat experts to sink their teeth into. Here's a roundup of the most critical vulnerabilities to date this year.

Read More

Dissecting Spring4Shell

Dissecting Spring4Shell

31.Mar.2022

Blueliv, an Outpost24 company

An RCE vulnerability affecting Spring Core's JDK 9 and later has become a trending topic in cybersecurity networks during the past couple days. This discovery, compared by some to the Log4Shell vulnerability, generated a lot of confusion and even got mistook with a different vulnerability affecting Spring Cloud, which got a CVE assigned the same day, and even linked them to completely unrelated commits on Spring Core's GitHub. In this blogpost, we will clarify what happened and what you can do to protect yourself.

Read More

Russian-linked malware cyberattacks

Russian-linked malware cyberattacks: what you need to know about Hermetic Wiper and Cyclops Blink

08.Mar.2022

Blueliv, an Outpost24 company

Just days after Russia launched its invasion against the people of Ukraine, news reports emerged of several cyberattacks. Deployed systematically ahead of the land invasion, Russian cyberattacks against Ukraine have rendered Ukrainian banks, government departments and other core services unavailable through the use of sophisticated ‘data wipers

Read More

mitre ATT&CK® framework

Using Mitre Att&CK with threat intelligence to improve Vulnerability Management

29.Nov.2021

Simon Roe, Product Manager Outpost24

Threat actors are constantly evolving their tactics and techniques in the attack lifecycle and infiltrate company infrastructure. While most organizations are already performing vulnerability management based on CVEs by MITRE, few have considered the powerful correlations between threat intelligence, CVEs and the ATT&CK® framework. In this blog we highlight the benefits of bringing them together to drive focused remediation and improve cyber defense.

Read More

The most critical vulnerabilities

[The most critical vulnerabilities right now – November 2021]

10.Nov.2021

Blueliv, an Outpost24 company

[Read More]

CVE-2021-41773

[CVE-2021-41773 – Apache web server Path traversal]

07.Oct.2021

This past Monday, October 4th, Apache disclosed a vulnerability introduced on Apache HTTP Server 2.4.49 known as CVE-2021-41773. At the same time, update 2.4.50 was released, fixing this vulnerability. The vulnerability allows an attacker to bypass Path traversal protections, using encoding, and read arbitrary files on the webserver’s file system. Both Linux and Windows servers running this version of Apache are affected.

Read More

published 1M credit cards

Insights about All World Cards and the published 1M credit cards

12.Aug.2021

Blueliv, an Outpost24 company

“All World Cards” is a new underground card shop created at the end of May 2021. The card shop went quite unnoticed until it caught the attention of the cybercriminal underground and the cybersecurity industry on August 2, 2021, by making publicly available one million compromised cards totally free of charge. All World Cards has currently listed for sale more than 2,7 million compromised cards.

Read More

2021 Web Application Security for Pharma and Healthcare

GET THE GUIDE >>

Upcoming Events

There are currently no upcoming events.