deepwatch

Deepwatch ATI 2023 Annual Threat Report

Observations, Metrics, Trends & Forecast from the Deepwatch Adversary Tactics & Intelligence Team

Deepwatch shares the key threats in our environment, the number of unique Deepwatch global detections, and the top engagements conducted by ATI threat hunters in 2022.

Top 5 ATT&CK Techniques

01 Exploitation

02 Initial Access

03 Persistence

04 Credential Access

05 Exfiltration

26,448 software security flaws were reported by CISA,

with the number of critical vulnerabilities (CVEs) up 59% from 2021.

Top 5 Threat Detections

1. Malware/Endpoint
2. Authentication
3. Intrusion Detection
4. Email/Phishing
5. Network

"Malware/Endpoint detections are the highest fidelity alert that something malicious has happened on the endpoint. Identifying malicious activity on the endpoint in a timely fashion is critical as this means this activity made it to the endpoint and could possibly move laterally in the environment."

Deepwatch ATI Analyst

Percentage of top incidents requiring response from Deepwatch ATI

50% SYSTEM EXPLOITATION

24% BEC/EAC

13% ACCOUNT COMPROMISE

7% RANSOMWARE

3% INSIDER THREAT

3% SUPPLY CHAIN

2022 Deepwatch ATI Observations

Exploitation of critical vulnerabilities for internet-facing systems with publicly available exploit code facilitated initial access into organizations.

Ransomware still continues to affect many industry sectors and **appeared not to favor targeting specific industries.**

Account compromise continues to be a Top Attack Vector.

Deepwatch identified multiple **SEO poisoning** attacks that led to **malware (Gootloader)** being downloaded.

Deepwatch responded to USB usage that led to malware infection **(Raspberry Robin)** in several environments.

High risk ports and services located in cloud environments are frequently discovered by Deepwatch ATI, which cybercriminals continue to target for exploitation.

Deepwatch ATI Global Detections chart

Here are the **Top 5 Global Detections** and their percentage of the total global detections for 2022. Global detections identify suspicious or malicious activity in the standard log sets across all Deepwatch customer environments.

Current global detections cover 100% of all MITRE ATT&CK tactics.

2023 Forecast

Prepare for **Infostealers, Source Code Exploitation,** and **Container Attacks**

Cybercriminals are poised to develop new information stealing malware to steal sensitive information, like browser password stores and cookies to gain initial access or sell on cybercriminal markets.

"We forecast a challenging year in which ransomware, code repository vulnerabilities, and misconfigured or exposed storage will increase business risk."

Deepwatch ATI Analyst

Why Deepwatch

Deepwatch is the leader in managed security services, protecting organizations from ever-increasing cyber threats 24/7/365. Powered by the Deepwatch SecOps platform, we provide the industry's fastest, most comprehensive detection and automated response to cyber threats together with tailored guidance from dedicated experts to mitigate risk and measurably improve security posture. The world's leading companies, from the Fortune 100 to mid-sized enterprises, trust Deepwatch to protect their business.

deepwatch

As a partner and extension of internal security teams, Deepwatch offers peace of mind and assurance that threats are rapidly and holistically addressed, unlocking a new level of security that supports business outcomes.

Get a Demo with **Deepwatch Security Experts**

Ready to Talk: **www.deepwatch.com**

© Copyright 2023 Deepwatch Incorporated. All Rights Reserved.