deepwatch

Deepwatch Threat Intelligence 2022

See Threats. Stop Breaches. Together.

Introduction

Intelligence is leveraged by governments and organizations around the world when making critical organizational decisions. Collecting data points to analyze for potential outcomes can transform these data points into Intelligence which tells a story that assists in key strategic, operational, and tactical decisions.

2021 Deepwatch Observations

- **Exploitation of Zero-day Vulnerabilities for Internet facing systems** with publicly available exploit code facilitated initial access into organizations. Significant Cyber events included Proxylogon, ProxyShell, and Log4j.
- Ransomware continued to affect many industry sectors and **appeared not to favor targeting of specific industries** over others
- Ransomware Threat Actors specialized their trade craft
    - **Initial Access Brokers,** Pentesters (Allifates), and Ransomware development (Ransomware Operators)
- Malware/Endpoint based alerts were the most frequent alerts
- Alerting activity increased during times of Significant Cyber Events
- **Increase in Ransomware Attacks which exfiltrated data** to hold for ransom (As opposed to encrypting an organization's data)

2021 Top 5 Threat

In 2021, the industry saw a transition into threat actor separation of duties, with an increase in groups focused on obtaining and selling access to victims (Initial Access Brokers). In fact, the Top 3 threat actors as tracked by Digital Shadows were all initial access brokers. This transition facilitates threat actor activities at scale. In observing this trend, Deepwatch has taken note of the proliferation of Initial Access Brokers and how it correlates with a shift in focus, away from specific industries and towards attacks of opportunity. As this trend continues, more emphasis must be placed on risk management of organizations' internet exposure

Both Digital Shadows Top 5 attack methods for 2021 and Deepwatch's data analysis support these observations.

Attack Methods

Source: Digital Shadows

- Remote Services
- Network Service Scanning
- Trusted Relationship
- Active Scanning
- Phishing

Threat Actors

Source: Digital Shadows

- nei (Initial Access Broker)
- barf (Initial Access Broker)
- inthematrix1 (Initial Access Broker)
- UNC2452 (Cyber Espionage Group)
- Astro Locker Team (MountLocker ransomware group)

Malware Variants

Source: Malwarebazar

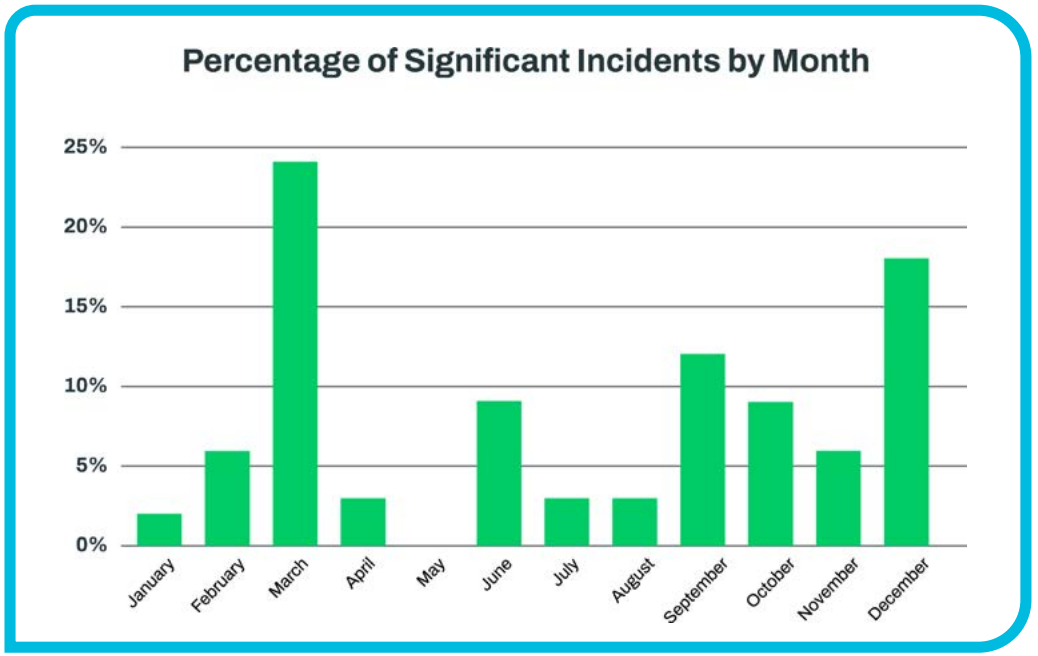
- Emotet (Heodo)
- Quakbot
- AgentTesla
- Dridex
- FormBook

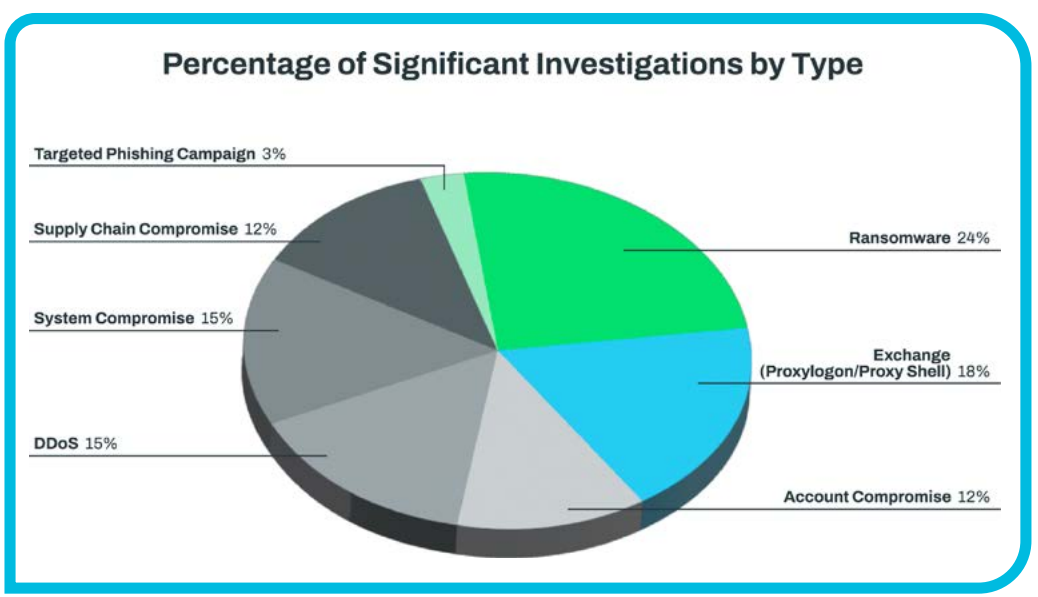
Significant Incidents

In 2021, deepwatch recorded 33 Significant Incident events. Due to the extent of the attacks, Significant Incident events require additional resources for investigation. Ransomware was the most prevalent event type and was closely followed by events involving exploitation of Microsoft Exchange (Proxy Logon" and "Proxy Shell"). Unsurprisingly, events spiked during or shortly after public disclosures of major vulnerabilities and exploit code releases. Specifically, March saw the Microsoft Exchange vulnerabilities being disclosed and December saw the Log4J disclosure.

Key Takeaway:

Monitoring for critical vulnerabilities and exploit code releases for those vulnerabilities and patching them in a timely matter should remain a top priority.





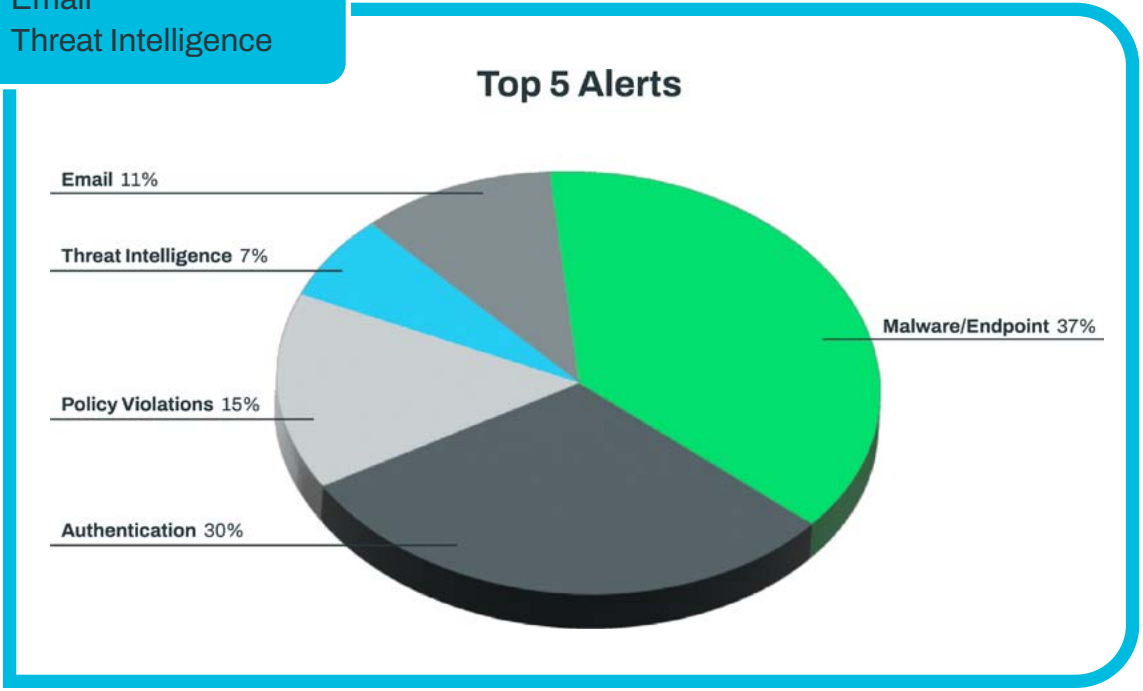
Top 5 Alert Types

The top alerting type for 2021 was Malware/ Endpoint alerts associated with activity occurring at the system level. Malware/Endpoint alerts are considered the highest-fidelity alerts due to detecting suspicious/malicious program execution on systems inside the environment. Notable Malware/Endpoint alerting activity observed in 2021 included malicious downloaders, password scrapers, post-exploitation tools, WebShells, ransomware, security protection termination tools, and banking trojans.

Authentication alerting was the second most prevalent. Many of these alerts focus on identifying suspicious/malicious authentication activities to systems or applications which is instrumental in identification of unauthorized authentication activities. As many organizations have recently expanded their external footprint to allow remote access of organizational resources, the importance of effective authentication alerts will continue to increase. Notable Authentication activities include Brute force login attempts, Password Spraying, Unusual authentications from locality or region, SSH Login attempts, and lateral movement authentication attempts.

Top 5 Alerts

1. Malware/Endpoint
2. Authentication
3. Policy Violations
4. Email
5. Threat Intelligence



Top 5 MITRE ATT&CK

MITRE ATT&CK offers a common nomenclature to facilitate analysis and discussion amongst cybersecurity professionals. While it is useful for this purpose and for understanding attacks, it is considerably less reliable as a detection coverage map due to the complexities of attack actions and shifting threat vectors.

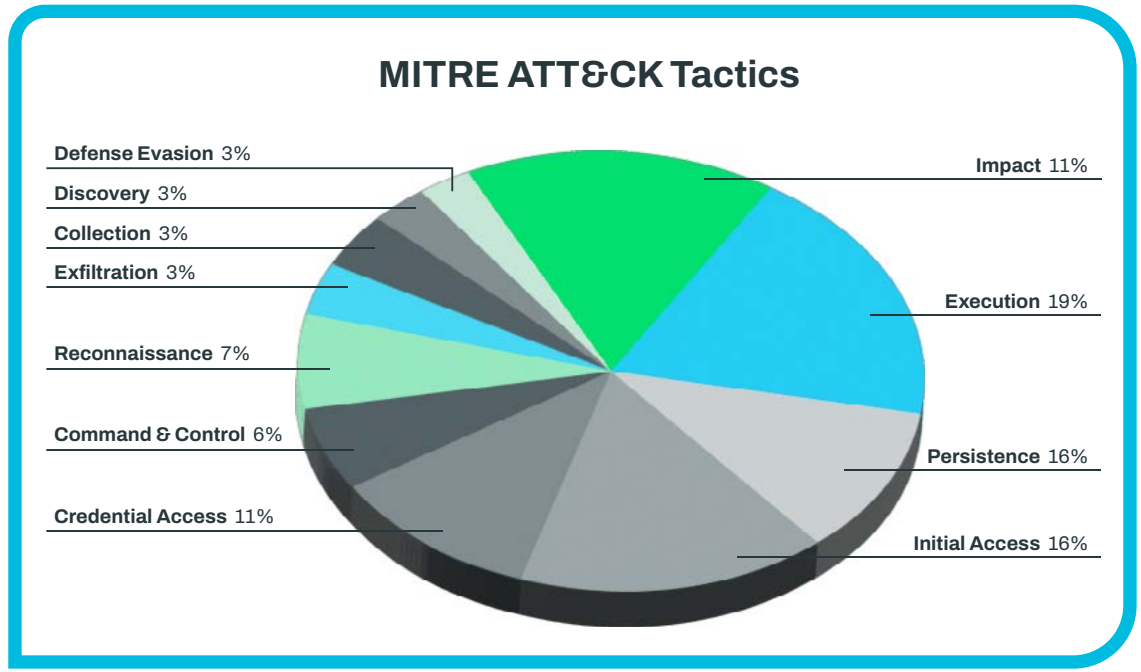
MITRE ATT&CK Tactics allow organizations to breakdown and categorize the different activities that Threat Actors conduct during their breach operations. Tactics are broken down further into Techniques and then into specific Procedures to make up the commonly referenced acronym known as TTPs. MITRE ATT&CK Tactics have been mapped to Deepwatch detection capabilities which could then be further analyzed or correlated together for a more comprehensive understanding of breach activities within an organization.

Top 5 MITRE ATT&CK Tactics

1. Executiton
2. Persistence
3. Initial Access
4. Credential Access
5. Impact

The most prevalent MITRE ATT&CK Tactic in 2021 for Deepwatch alerts was Execution which mapped to 19% of all alerts. Execution is associated with attacker controlled code execution on a local or remote system. Some Techniques included under Execution are Command and Scripting execution, User execution of malicious files or links, abuse of native system components, and malicious service installation execution.

The second most frequent Tactic observed was Persistence at 16%. Persistence activities are associated with attackers attempts to maintain a foothold on the systems. Techniques associated with Persistence include Account Manipulation, Autostart Executions and Scripts, Backdoor Server Software Components like WebShells, and Scheduled Tasks execution.

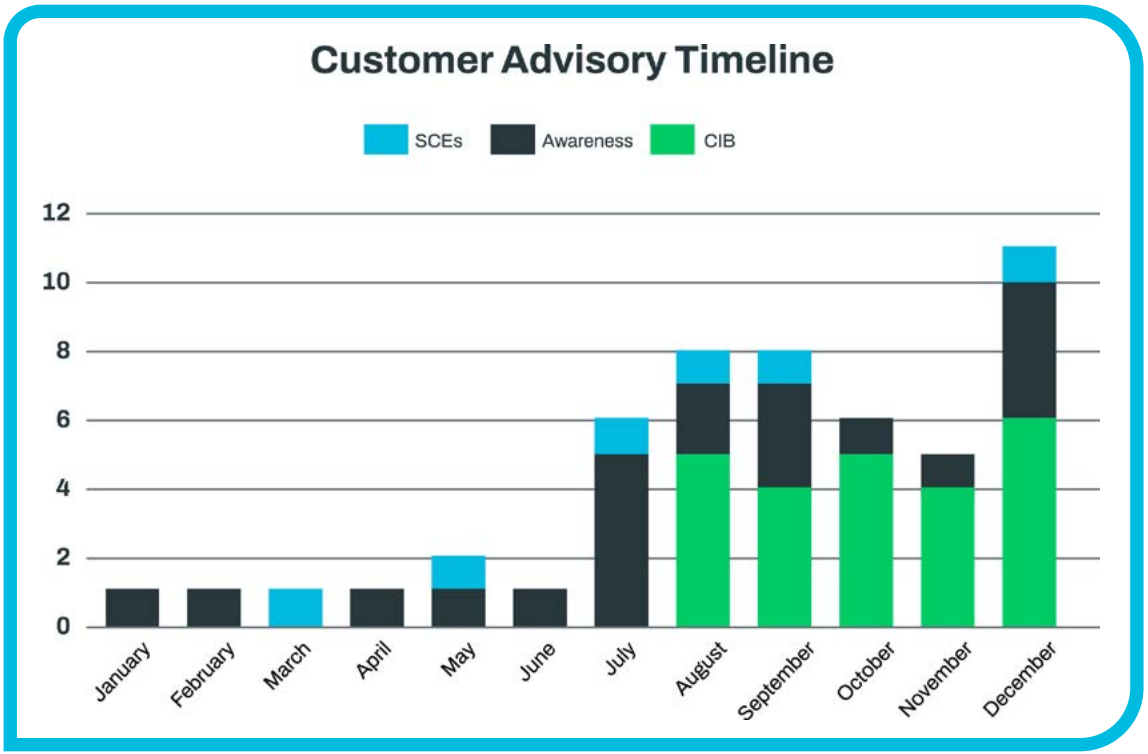


Threat Intel Reports Metrics & Trends

Threat Intel Team published 50 reports in 2021.

The majority of significant cyber events in 2021 involved critical vulnerabilities in widely used software being exploited in the wild. Frequently, the vulnerable software was internet facing in organizations' environments.

Signalling an increased need for organizational focus on perimeter risk.



Cyber Intelligence Brief	Customer Advisory Awareness	Customer Advisory SCE
24	20	6

2022 Outlook

- **High confidence that Ransomware Threat Actors** will continue to take advantage of opportunities rather than target specific industry sectors
- **High confidence that Critical Zero-day** vulnerabilities with publicly available exploit code for popular Internet facing technologies will continue to be uncovered
- **High confidence that Threat Hunting** activities will uncover threats in organizations that were not prevented or detected by endpoint security products
- **Moderate confidence that alert** volume and fatigue will lead to more missed incidents, unless a focus is placed on higher fidelity alerting in the industry
- **Moderate confidence that an increase** in lower skilled Ransomware operators will be observed as Threat Actors specializing in Initial Access continue to obtain and sell access to the highest bidder

How To Get Threat Ready 2022

Deepwatch recommends asking your security team these questions:

Need help?

Reach out to your Squad Manager for advisement on getting ready for 2022.

What does our organization's Internet-facing footprint look like?	Deepwatch offers an external profile engagement to identify systems and services that are Internet-facing and potentially susceptible to attack
Does our patch management strategy focus on prioritizing Internet-facing systems/technologies?	Deepwatch offers Vulnerability Management (VM) services to organizations incorporating a priority patching process for Internet facing systems and software
Do we have MFA for externally accessible high-risk business services like Email or Remote Access?	Deepwatch can partner with your organization to identify single-factor services or remote access software through our external profile offering
What is our plan to review our external systems security configurations for hardening improvements?	Deepwatch offers Vulnerability Management (VM) services that includes secure configuration recommendations
Is our endpoint protection/detection software functioning properly?	Deepwatch offers Managed Detection and Response (MDR) services for 24/7 coverage to ensure protection and detection technologies are functioning and reporting properly
Have we reviewed, updated, and tested our incident action plans?	Deepwatch offers security consulting services to assist in building, updating, and testing incident actions via table top exercises

deepwatch

ABOUT DEEPWATCH

Deepwatch helps secure the digital economy by protecting and defending enterprise networks, everywhere, every day. Deepwatch leverages its highly automated cloud-based SOC platform backed by a world class team of experts who monitor, detect, and respond to threats on customers' digital assets 24/7/365. Deepwatch extends security teams and proactively improves cybersecurity posture via its Squad delivery and patented Security Maturity Model. Many of the world's leading brands rely on Deepwatch's managed detection and response security.

Visit www.deepwatch.com or reach out to us at sales@deepwatch.com.