



CYBER SECURITY

Introduction

Reading Time: 11 minutes

Cyber-attacks have continued to grow with the advent of technologies that are available, to break into systems and networks. Findings from IBM indicate that it takes a company 197 days to discover the breach and up to 69 days to contain it. There have been many incidences of attack on critical infrastructures such as healthcare, water systems, and power grids etc. On a smaller scale, there has been a spurt in ransomware and malicious software attacks on enterprise networks.

Recent news

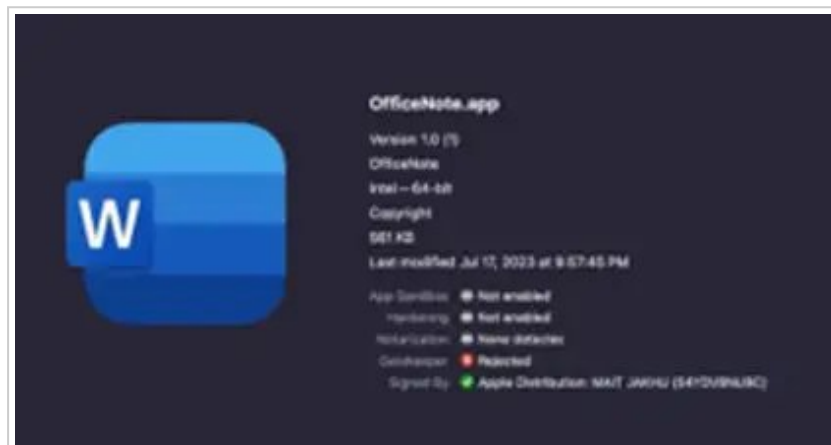
A cyber espionage campaign dubbed Operation Jacana was launched to target the governmental entity in Guyana which was detected by ESET in February 2023 It included a spear-phishing attack that resulted in the deployment of an undocumented implant written in C++ called DinodasRAT.





The attack began with a spear-phishing email containing a malicious link referencing a news report about a Guyanese fugitive in Vietnam. Clicking the link downloaded a ZIP archive file from a compromised Vietnamese governmental website, launching the DinodasRAT malware.

A new variant of macOS malware, named XLoader, has emerged. Disguising itself as the “OfficeNote” productivity app, XLoader is an information-stealing and keylogging malware that bypasses previous limitations by using different programming languages. It was detected by Sentinel One researchers, indicating an active campaign. The

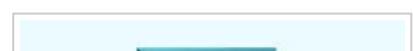


malware installs in the background, targeting clipboard data and browser information, with persistence tactics. Offered on forums for rent, this iteration aims at macOS users in work settings, underscoring the ongoing threat of XLoader. Vigilance and strong cybersecurity measures remain crucial for macOS protection.

Software provider Ivanti has warned of active exploitation of zero-day flaw in Ivanti Sentry (CVE-2023-38035), enabling unauthorized access due to weak configuration. Attackers could manipulate settings and execute commands. Risk is lower if port 8443 is not exposed online. Vulnerability could leverage other flaws (CVE-2023-35078, CVE-2023-35081). mnemonic credited for discovery.



CISA added critical Adobe ColdFusion flaw (CVE-



2023-26359) to its exploited vulnerability catalog due to active attacks. The flaw allows arbitrary code execution. Patched by Adobe in March 2023, the specifics of exploitation are unclear.



A high-severity WinRAR flaw (CVE-2023-40477) allows remote code execution on Windows systems. Improper validation of recovery volumes leads to memory access beyond allocated buffer, enabling attackers to execute code in current process. Exploitation involves user interaction via malicious page or archive file. Discovered by goodbye Selene, users are urged to update to latest version



The practical effectiveness of Zero Trust is tested by Advanced Persistent Threats (APTs), as shown in the Storm-0558 hack targeting government agencies. The attackers used fake authentication tokens to access Microsoft Outlook accounts. Zero Trust is embraced by organizations, relying on continuous verification and dynamic control for users and devices. Network analysis tools like Network Detection and Response (NDR) are key for effective Zero Trust implementation, as traditional systems can falter. NDR, particularly with Machine Learning, detects anomalies and enhances security. ExeonTrace, a leading NDR solution, utilizes ML for network visibility and incident response, reinforcing Zero Trust cybersecurity strategies.

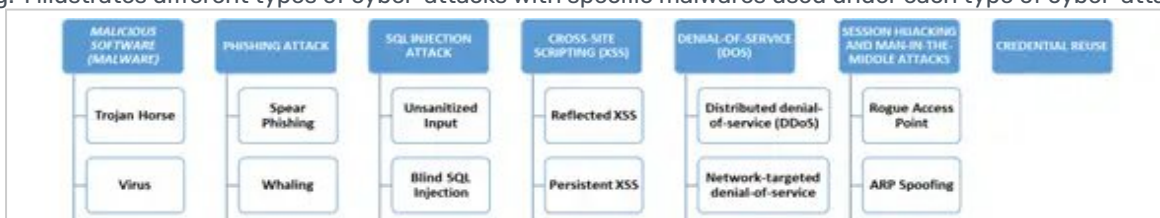


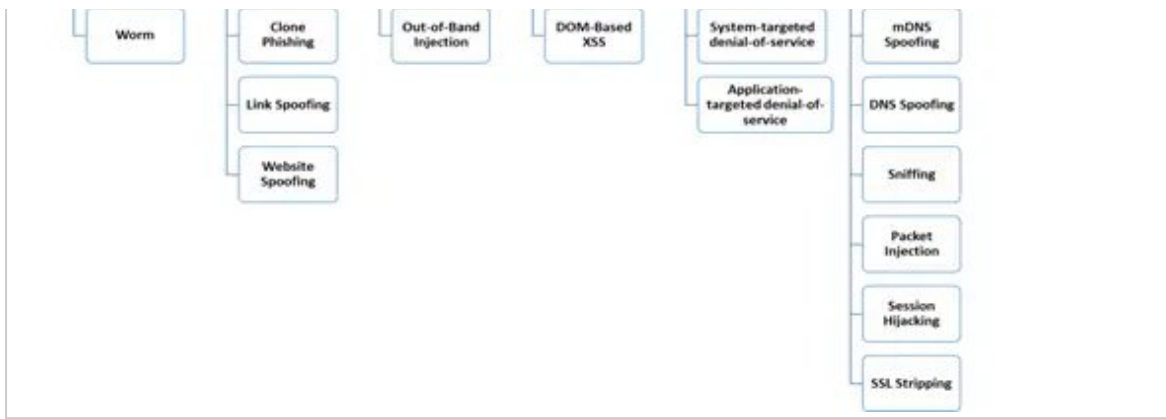
TYPES OF CYBER ATTACKS

The most common cyber-attacks on small businesses include:

- Phishing/Social Engineering (57%)
- Compromised/Stolen Devices (33%)
- Credential Theft (30%)

Fig. 1 illustrates different types of cyber-attacks with specific malwares used under each type of cyber-attack.





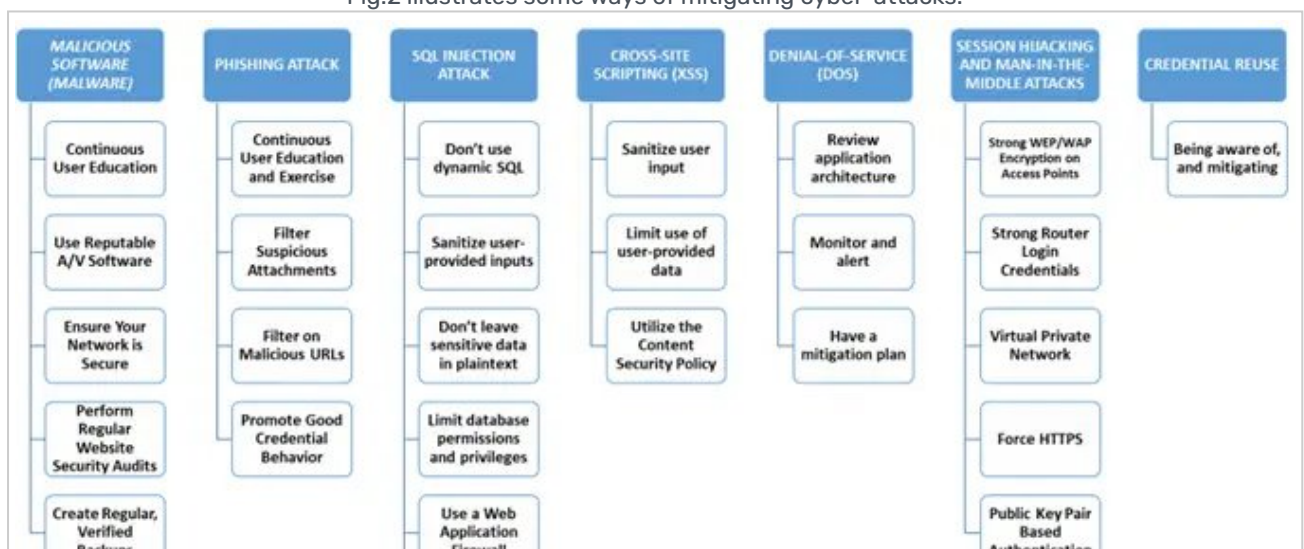
In August 2022, the website of the Finnish parliament encountered a significant cyber incident in the form of a Distributed Denial-of-Service (DDoS) attack, coinciding with an ongoing parliamentary session.

In July 2022, the Belgian government disclosed that it had been subjected to targeted cyber intrusions. Specifically, three distinct Chinese hacker groups, affiliated with established Chinese Advanced Persistent Threat actors, launched sophisticated attacks against Belgian public services and military defense entities. These state-sponsored Chinese threat actors engaged in the illicit acquisition of trade secrets and sensitive intelligence information. Notably, the Soft Cell Chinese group, operating within this context, introduced a novel remote access trojan (RAT) malware variant in June 2022.

PREVENTION OF CYBER ATTACKS

Basic precautions can be taken to prevent cyber-attacks- namely, shrinking data transfers, downloading sensibly, monitoring data leaks, updating device software on time, developing a breach response plan and improving password security.

Fig.2 illustrates some ways of mitigating cyber-attacks.





CYBER SECURITY ANALYTICS

The global cyber threat continues to evolve at a rapid pace, with an increasing number of data breaches each year. A report by Risk Based Security revealed that a shocking 100 billion records have been exposed by data breaches, and more than 1.5 billion records have been exposed by data breaches during the first half of 2022 alone.

Fig. 3 illustrates technologies that thwart cyber security threats / attacks.



TECHNOLOGIES

There is a need to acknowledge cybercrimes, treat them seriously and have preventive measures in place. A cybercrime's prime objective is no more just vengeance, quick money or extracting confidential details. It has transformed into bigger targets and more sinister motives, commonly known as cyber warfare.

All critical infrastructures such as utility services, nuclear power plants, healthcare facilities, airports, etc. are connected to a network. In fact, all the companies have their business-critical data recorded in digital format and are greatly dependent on their systems and networks. In such circumstances, even a small attack on the network or system can have a great effect on their operations. Failure to protect any such critical networks from potential cyberattacks can put risk on credibility, sales, profits, and sometimes, even national security.

Technologies used to predict threats and enhance cyber security systems are presented in Fig. 4.



Fig.4

Artificial Intelligence & Deep Learning

Artificial Intelligence (AI) is being considered as the primary solution provider to address cybersecurity issues. AI technologies deeply analyze systems and keep a real-time check on everything that we perform. It analyzes every small action and this helps to protect systems from threats. AI technologies such as machine learning (ML) and natural language processing (NLP) enable analysts to respond to threats with greater confidence and speed. AI is trained by consuming billions of data sets from both structured and unstructured sources such as blogs and news stories. Through machine learning and deep learning techniques, AI is trained to understand cybersecurity threats and cyber risk.

AI collects information and uses reasoning to identify the relationships between threats, such as malicious files, suspicious IP addresses or insiders. This analysis takes very less time, say just a few seconds or minutes, allowing security personnel to respond to threats immediately. AI eliminates time-consuming research tasks and provides accurate risk analysis. It reduces the amount of time that the security personnel take to make the critical decisions and launch an organized response to remediate the threat. Many big companies have developed their own AI technology to operate their system without any unauthorized interruptions.

Vulnerability Management

The AI-based systems which are highly proactive in detecting the vulnerabilities can analyze patterns and discover loose ends that can be potentially vulnerable. By recognizing the attackers' pattern, infiltrating methods can be identified, and so it becomes easy to anticipate when and how any vulnerability would make its way to the network or system.

Improving the Authentication

Modern biometric authentication methods such as face recognition, iris recognition, and login authentication have made systems highly secure. The use of AI in biometrics has made it difficult for cybercriminals to hack systems.

Behavioral Analytics or UEBA (User and entity behavior analytics)

Behavior analytics in cybersecurity involve use of software tools to detect patterns of data transmissions in a network that are not normal. The anomaly would be detected by the analytics tool and alert IT managers, who would quickly stop the cyberattack. This is the programming system that analyzes or keeps a watch on the actions that we perform on a specific platform. Facebook, Instagram, and other social media platforms use this program. Such behavioral analytics are used by enterprises to detect intrusions that elude preventive technologies such as firewalls, intrusion-prevention systems, and antivirus software. While conventional tools match fingerprints or signatures identified in previous attacks, behavioral analytics tools study and report anomalies that are compared to a baseline of normal behavior.

UEBA is a very important component of IT security, allowing one to detect:

- **Insider threats:** It is not too far-fetched to imagine that employees could go rogue, stealing data and information by using their own access. UEBA can help detect data breaches, sabotage, privilege abuse, and policy violations caused by one's own staff.
- **Compromised accounts:** Sometimes, user accounts could become compromised because of the user unknowingly installing malware on their machine, or if, sometimes, a legitimate account is spoofed. UEBA can help isolate spoofed and compromised users before they can do real harm.

- **Brute-force attacks:** Cloud-based entities and third-party authentication systems may also be targeted by hackers. With UEBA, one can detect brute-force attempts, and help block access to these entities.
- **Changes in permissions and creation of super users:** ~~Some attacks involve the use of super users.~~ UEBA allows one to detect whenever super users are created thereby avoiding attacks by them, or if unnecessary permissions are granted to accounts.
- **Breach of protected data:** It is not enough to just keep the protected data secure. It is also important to know if an access is made by a user when there is no legitimate business reason to access the data.

Embedded Hardware Authentication

A PIN and password are just not enough to protect hardware anymore. More frequently, people are experiencing their accounts being operated by unknown entities. Embedded authenticators are now being used to verify a user's identity.

Intel has demonstrated a breakthrough in this domain by introducing Sixth-generation vPro Chips, which are powerful user authentication chips that are embedded into the hardware itself. The system has multiple organized sets of authentication and levels to secure the device or software. This advanced technology has opened new doors for a secure mode. Intel Authenticate uses a combination of up to three hardened factors at the same time to verify identities: "something you know," such as a personal identification number; "something you have," including a mobile phone; and "something you are," such as a fingerprint. End users can combine factors such as phone proximity, to enable Network Access to log in to domains and VPNs, and "Walk-Away Lock," which uses presence technology to lock a system when users leave their PC unattended. IT can choose from multiple hardened factors of authentication that are based on company policies, and no longer need to rely solely on employees remembering complicated passwords.

Blockchain Cybersecurity

Blockchain cyber security is one of the latest technologies that is gaining momentum and recognition as a promising mitigation technology for cybersecurity.

Blockchain technology has been designed to be transparent. While offering data security, it is also aimed at maintaining the integrity of the transactions, not its privacy. The responsibility for verifying the authenticity of the data added lies with every member in a blockchain. Blockchains create a near-impenetrable network for hackers and are currently one's best bet to safeguard data. Therefore, the use of blockchain with AI can establish a robust verification system to keep potential cyber threats at bay.

Securing Private Messaging: Most messaging companies are using blockchain for securing user data as it is a better option to the end-to-end encryption which is currently in use. In the recent past, numerous attacks have been witnessed against social media platforms such as X and Meta. These attacks have caused data breaches with millions of accounts being breached and user information landing in wrong hands. Blockchain technologies, if implemented properly in these messaging systems, may prevent future cyberattacks.

IoT Security: Edge devices, such as thermostats and routers, are also being used by hackers to gain access to overall systems. Taking advantage of the popularity of AI, hackers have been accessing overall systems such as home automation through edge devices like 'smart' switches. In most cases, many these IoT devices have sketchy security features. In such cases, blockchains can be used to secure such overall systems or devices by decentralizing their administration. The approach will enable the device to make security decisions on its own. The edge devices have become more secure by quickly detecting and acting on suspicious commands from unknown networks without depending on the central admin.

Securing DNS and DDoS: When users of a target resource, such as a network resource, server, or website, are denied access or service to the target resource, a Distributed Denial of Service (DDoS) attack occurs. These attacks harm the resource systems by shutting or slowing them down.

Comparatively, an intact Domain Name System (DNS) is much centralized, making it a perfect target for hackers who infiltrate the connection between the IP address and the name of a website making the website inaccessible,

cashable, and even redirectable to other scam websites. Block chain can be used to diminish such kinds of attacks by decentralizing the DNS entries.

Decentralizing Medium Storage: While business data hacks and theft are becoming a primary cause of concern, most organizations still use the centralized form of storage medium. To access the data stored in these systems, a hacker simply exploits a single unguarded point. Such an attack leaves sensitive and confidential data, in the possession of an offender. By using block chain, sensitive data may be protected by ensuring a decentralized form of data storage. This mitigation method would make it tough for hackers to penetrate data storage systems.

The Provenance of Computer Software: Block chain can be used to ensure the integrity of software downloads to prevent foreign intrusion. Just as the MD5 hashes are utilized, block chain can be applied to verify activities, such as firmware updates, installers, and patches, to prevent the entry of malicious software in computers.

However, in the case of block chain technology, the hashes are permanently recorded in the block chain. The information recorded in the technology is not mutable or changeable; hence block chain may be more efficient in verifying the integrity of software by comparing it to the hashes against the ones on the block chain. **Verification of Cyber-Physical Infrastructures:** Data tampering, systems misconfiguration along with component failure have harmed the integrity of information generated from cyber-physical systems. However, the capabilities of block chain technology in information integrity and verification may be utilized to authenticate the status of any cyber-physical infrastructures. Information generated on the infrastructure's components through block chain can be more assuring to the complete chain of custody.

Protecting Data Transmission: In future, block chain technology can prevent unauthorized access to data while in transit. Through complete encryption, data transmission can be secured thereby preventing individuals or organizations from accessing the data.

Diminish Human Safety Adversity caused by Cyber-attacks: Innovative technological advancements have recently seen the roll-out of unmanned military equipment and public transportation. This has been made possible by

the Internet that facilitates transfer of data from sensors to remote databases. However, hackers can break in and gain access to networks, such as Car Area Network (CAN). When accessed, the hackers can gain complete control of vital automotive functions. Such incidents may compromise the safety of humans. But through data verification conducted on block chain for any data that goes in and through such systems, many adversities could be prevented.

Internet of Things (IoT)

Increasingly more objects and systems in our lives are becoming embedded with network connectivity and computing power in order to facilitate communication with similarly connected devices or machines. Expanding networking capabilities to all corners of our lives can make us more efficient, help save time and money, and put our digital lives at our fingertips whenever we need it.

Business and government sectors too have also joined the IoT bandwagon. Healthcare has seen huge benefits from patient wearables that monitor vitals and feed valuable information to the healthcare professionals. Manufacturing and industrial sectors have also seen wide adoption of IoT in Industrial Control Systems (ICS) such as SCADA Systems.

The more devices we connect in our lives, the more entry points we make available to threats. When a fridge becomes internet-enabled it can be hacked by cyber criminals, same as a phone or laptop. As the expansion of the IoT market continues, so will the number of potential risks that threaten the performance and safety of devices and the integrity of IoT data.

Internet of Threats

Companies across industries are deploying IoT solutions for improved efficiencies and to garner higher level of visibility. Hackers constantly devise new ways to compromise systems and gain access to data, resulting in navigation systems on connected vehicles or smart medical devices, or any IoT system to become compromised due to hacking.

Securing the IoT Ecosystem

Securing IoT devices is a big challenge. While manufacturers and innovators roll out new products, in the race to reach the market first, security is compromised. Many businesses may not be aware of the vulnerabilities that IoT presents, and this could cause problems.

Be it national power generation and distribution infrastructures or global manufacturing operations, connected IoT sensors and devices can significantly increase operational risks. Besides securing individual IoT devices, organizations also need to ensure that their IoT networks are secure. Thus, it is important to enable only authorized users to gain access to the IoT framework and access control mechanisms, which can be achieved with the help of strong user authentication.

Big Data

The age of big data and cyber security provide both challenges and opportunities for businesses. While big data has opened new possibilities in terms of analytics and security solutions to protect data and prevent cyber-attacks, it has also given cyber criminals the opportunity to access huge amount of sensitive and personal information.

Three main challenges to businesses poised by big data:

- Protecting sensitive and personal information
- Data rights and ownership
- Not having the talent (i.e., data scientists) to analyze the data

While addressing the main challenge of safeguarding information may sound simple, the scale of data that needs to be processed and analyzed in order to prevent cyber-attacks, makes it daunting. According to Computer World, a medium-size network with 20,000 devices (laptops, smartphones, and servers) will transmit more than 50 TB of data during a 24-hour period. This translates to over 5 GBits that needs to be analyzed every second to detect cyber-attacks, potential threats, and malware.

Big data analytics provide cyber security professionals the opportunity to analyze different types of data from various sources and then respond in real time. Big data analytics enables connecting the dots between vast amount of

data that is collected from the vast universe, making correlations and connections that may have otherwise been missed.

The benefits offered by big data to businesses are:

- Business intelligence through access to vast data/customer analytics which will help enhance and optimize sales and marketing strategies
- Fraud detection and a Security information and event management (SIEM) systems replacement

Enhancing Big Data Security

Targeting big data sets often has its own pay-offs for cyber criminals. They have a lot to gain when they go for such a large data set. The companies have a lot to lose when they face a cyber-attack without proper security measures in place.

In order to increase the security around big data, businesses may consider:

- Collaborating with other industry peers to create industry standards, and share best practices
- Attribute-based encryption to protect third-party information
- Hadoop-like secure open-source software
- Maintain and monitor audit logs across all aspects of business

Zero-Trust Model

The Zero Trust model assumes breach and verifies each request as though it originates from an open network instead of assuming that everything behind the corporate firewall is safe. Zero Trust banks on the policy of “never trust, always verify,” regardless of the origin of the request.

Main principles and technologies behind zero trust security

- Attackers exist both within and outside of the network, so no user or machine can be taken for granted.
- Least-privilege access – this means giving users only as much access as they need, like an army general giving soldiers information on a need-to-know basis.

- Micro segmentation, or breaking up security area into small zones to maintain separate access for separate parts of the network. For example, a network with files living in a single data center that utilizes micro segmentation may contain dozens of separate, secure zones. Without separate authorization, a person or program with access to any one of those zones will not be able to access any other zone.

Multi-factor authentication (MFA), requiring more than one piece of evidence to authenticate a user; just entering a password is not enough to gain access. A commonly seen application of MFA is the 2-factor authorization (2FA) used on popular online platforms such as Facebook and Google. With every access request fully authenticated, authorized, and encrypted before granting access, it requires users who enable 2FA for these services to not only enter a password but also enter a code sent to another device, such as a mobile phone, thus providing a two-fold evidence of who they claim to be.

CRITICAL IMPLICATIONS

Hospitals

In the year 2020 a patient died when the IT systems in a German hospital were hacked. While originally the hackers had planned to attack Heinrich Heine University, the systems of the affiliated Düsseldorf University Clinic were brought down by mistake. The attack encrypted 30 servers at the hospital, and left a ransomware note addressed to the university. With systems down, patient data inaccessible, and operations postponed, the patient had to be sent to a different hospital an additional 20 miles away, delaying potentially life-saving treatment.

Power Grid

The massive power outage in October 2020 in Mumbai, India, left railways, stock market, hospitals, and a population of 20-million in Mumbai high and dry for several hours. The US cybersecurity firm Recorded Future claimed that the China-backed Red Echo group targeted India's power grid.

e-commerce

Hackers from China's Guangdong and Henan provinces targeted millions of

Indian online shoppers during the festive months of October and November, 2020. Chinese hackers launched 'Spin the lucky wheel scam' within days of Flipkart announcing the Big Billions of Days sale and later created a similar-looking fraud 'Amazon Big Billion Day Sale.' The hackers created fake URLs disguised as offers by Flipkart and Amazon and lured the netizens to click on them with bogus prizes. These links were disseminated through WhatsApp targeting many online shoppers in India. The information collected via these scams could be used to undertake more such cyber-attacks, especially targeted at internet users in Tier-II and Tier-III cities where awareness about such scams is low.

STARTUPS

Many startups all over the world are currently working on developing security solutions, some of which are presented below:

Founded in 2015, Bangalore-based AppSecure uses real-world hacking techniques to understand customers' security posture, discovering security vulnerability, and assisting their teams in fixing them. AppSecure was started with an objective to protect businesses, startups and companies from data breach and business losses due to security vulnerabilities in their internet assets.



Founded in 2019, California-based Axis Security's Application Access Cloud™ offers a new agentless model that connects users online to any application, private or public, without touching the network or the apps themselves. The company has its R&D center in Tel Aviv, Israel.



Founded in 2018, California-based DataFleets provides data scientists and developers with a "data fleet" that allows them to create analytics, ML models and applications on susceptible data sets without direct access to the data. Each data set has easy-to-use APIs and under-the-hood, which ensure data protection using advances in federated computation, transfer learning, encryption and differential privacy. DataFleets helps organizations by maintaining data protection standards for compliance while accelerating data



science initiatives.

Founded in 2019, California-based Orca Security integrates cloud platforms as an interconnected web of assets, prioritizing risk based on environmental context. Delivered as SaaS, Orca Security's SideScanning™ technology reads cloud configuration and workloads' runtime block storage out-of-band, detecting vulnerabilities, malware, misconfigurations, lateral movement risk, weak and leaked passwords, and unsecured PII.



Founded in 2018, Perimeter 81 was conceived with the aim of providing companies with the privilege of seamless network security management via a unified service delivered entirely from the cloud. Perimeter 81 delivers the same by offering multiple advanced security features.



Perimeter 81 is particularly adept at Secure Access Service Edge (SASE) and Zero Trust Network Access (ZTNA).

Founded in 2013, **Kratikal** offers cyber-attack simulation and awareness tools, anti-phishing, fraud monitoring & take-down solution, email authentication and anti-spoofing solution, phishing incident response, risk detection & threat analysis and code risk review.



Founded in April 2017, **WiJungle** offers a Unified Network Security Gateway, enabling organizations to manage and secure their entire network through a single window.



In 2018, WiJungle was recognized among the Most Innovative Product of the Year 2018 by the Data Security Council of India. With clients across 25+ countries, the cybersecurity startup serves government and private giants across industry verticals like defence, BFSI, hospitality, healthcare, education, retail, ITES, etc.

COMPANIES

There are many companies such as ScienceSoft, Hackerone, Intruder,

Symantec, Check Point, and Cisco operating within the cybersecurity sector with each one offering a range of core cybersecurity services and technologies to address various aspects of cybersecurity threats. They are not only working towards securing digital environments but also providing valuable solutions to combat the evolving challenges posed by cyber threats.

INTERESTING PATENTS

A few interesting patents that were either filed or granted recently are listed below.

US11522900B2 titled System and method for cyber security threat assessment assigned to BitSight Technologies relates to a method by which traces of activities of online users who are associated with an entity are received from disassociated sources including a shared service servicing multiple entities; and inferring, by analysis of the traces of the online users' activities and a use of the shared service, a security of rating for the entity. The analysis comprises a comparison of traces that originated in different contexts of online activities, a context of the security of which is controlled or uncontrolled by the entity, wherein the context comprises a computer system or device made accessible by the entity to the user.

US11522901B2 titled Computer security vulnerability assessment assigned to Opswat Inc. relates to a method for receiving product binary data that includes hashes of strings of bits, bytes, words or characters extracted from a file of a product; and identification data for the same; receiving product vulnerability data and its identification; determining the correspondence between the binary data and the vulnerability data, wherein the product vulnerability data includes a country of origin for the product; generating, a binaries-to-vulnerabilities database based on a determined correspondence between the binary data and the vulnerability data; scanning, target to find matches between the binary data of the target and product and determining a known security vulnerability which includes the country of origin based on the above results.

US11522890B2 titled Network application security policy generation assigned to Zscaler Inc. relates to a method for receiving flow objects from computer

systems, wherein each flow object is data based on communication associated with the application; matching the flow objects when they represent two corresponding flows at opposite ends of an application-to-application communication; utilizing an evolutionary algorithm or a greedy algorithm to window down a set of rules; and generating the network communication model based on the match data wherein the model contains the winnowed set of rules resulting from the initial set of rules and is in a readable and modifiable form, and is configured to label a particular communication as permitted or blocked.

US11522832B2 titled Secure internet gateway assigned to Target Brands Inc. relates to a system comprising production secure gateways and each use datasets to determine how to process messages between devices on a network and websites on the internet. A version control server in the system automatically sends a dataset to secure gateway wherein it loads the dataset on a test secure gateway, wherein the test secure gateway is configured in an identical manner to each production secure gateway which communicates with internet websites, and the version control server automatically institutes testing on the test secure gateway that sends internet traffic and utilizes each port exposed by the test secure gateway for handling internet traffic.

US11520655B1 titled Systems and methods for self-correcting secure computer systems assigned to Keep Security LLC relates to A self-correcting secure computer system comprising a ROM, a RAM, and a processor in communication with RAM and ROM, programmed to receive an activation signal; retrieve data from ROM and execute on RAM the first configuration, store a key at a first memory location; execute a network connection; receive a request to access the key; deactivate the network connection; retrieve the key from the first memory location to volatile memory; perform operation with the key; delete the key from the volatile memory; and reactivate the network connection.

US11520873B2 titled Enrollment of a device in a secure network assigned to Electricite de France relates to a method for enrolling a first device in a secure network to which an information system is connected comprising steps implemented by a trusted device connected to the secure network: receiving from a user terminal, an authorization notifying the trusted device that the first

device is authorized to connect to the secure network wherein the connection authorization issued is conditional on the user of the terminal supplying a hardware cryptographic token and validating the same; generating cryptographic keys, and transmitting the cryptographic keys to the first device, so that it can communicate via the secure network without requiring further communication with the trusted device.

CONCLUSION

The escalating frequency and sophistication of cyberattacks has been posing significant threats to our increasingly digital world. As newer technologies emerge, so do the tools for cybercriminals to exploit vulnerabilities within systems and networks. Critical infrastructures such as healthcare, water systems, and power grids, along with enterprises, are prime targets for cyberattacks that can have dire consequences on operations, credibility, and even national security. Nation-state actors are increasingly engaging in cyber warfare, highlighting the transformation of cybercrime from mere financial motives to more sinister agendas. The rapid growth of the Internet of Things (IoT) contributes to the expansion of attack surfaces, with IoT cyberattacks expected to double by 2025. The need for enhanced cybersecurity measures is evident, with AI, behavior analytics, and blockchain emerging as potential solutions. As technology continues to advance, the urgency to counter cyber threats grows even stronger. The collaborative efforts of governments, businesses, and cybersecurity professionals are paramount to securing our digital future and mitigating the potential harm posed by cybercriminals.

REFERENCES

- <https://thehackernews.com/2023/10/guyana-governmental-entity-hit-by.html>
- <https://thehackernews.com/2023/08/new-variant-of-xloader-macos-malware.html>
- <https://thehackernews.com/2023/08/ivanti-warns-of-critical-zero-day-flaw.html>
- <https://thehackernews.com/2023/08/critical-adobe-coldfusion-flaw-added-to.html>
- <https://thehackernews.com/2023/08/critical-adobe-coldfusion-flaw->

added-to.html

- CYBERSECURITY TRENDS IN 2020 & THE THREATS FACING THE INDUSTRY
<https://blog.eccouncil.org/cybersecurity-trends-in-2020-the-threats-facing-the-industry/#:~:text=Ransomware%20and%20malware,continue%20to%20skyroc>
- How are Emerging Technologies Changing the Cyber Security Landscape
https://medium.com/@hemang_rindani/how-are-emerging-technologies-changing-the-cyber-security-landscape-af207303ba22
- The 5 Latest Cyber Security Technologies for Your Business
<https://ifflab.org/the-5-latest-cyber-security-technologies-for-your-business/>
- The 10 Top Cybersecurity Startups Of 2019 (So Far)
<https://www.crn.com/slide-shows/security/the-10-top-cybersecurity-startups-of-2019-so-far-/11>
- Top 30 BEST Cyber Security Companies In 2020 (Small to Enterprise Level Firms)
<https://www.softwaretestinghelp.com/best-cyber-security-companies/>
- The Future Use Cases of Blockchain for Cybersecurity
[https://www.cm-alliance.com/cybersecurity-blog/the-future-use-cases-of-blockchain-for-cybersecurity#:~:text=Blockchain%20technology%20is%20a%20distributed,computers.&text=The%20new%20technology%20is%20considered,in%20the%](https://www.cm-alliance.com/cybersecurity-blog/the-future-use-cases-of-blockchain-for-cybersecurity#:~:text=Blockchain%20technology%20is%20a%20distributed,computers.&text=The%20new%20technology%20is%20considered,in%20the%20)
- Cybersecurity
<https://builtin.com/cybersecurity>
- <https://www.analyticsinsight.net/impact-of-artificial-intelligence-in-cyber-security/>
- <https://www.computerworld.com/article/3147017/behavior-analytics-tools-for-cybersecurity-move-into-enterprises.html#:~:text=Behavior%20analytics%20in%20cybersecurity%20is,t>
- <https://analyticsindiamag.com/can-india-stand-up-to-chinas-cyber-warfare/>
- <https://www.timesnownews.com/business-economy/industry/article/chinese-launch-covert-cyber-attacks-on-india-millions-of-online-shoppers-targeted/696678>
- <https://dzone.com/articles/cybersecurity-technologies-you-should-be-aware-of>

- <https://www.educba.com/types-of-cyber-security/>
- <https://www.cm-alliance.com/cybersecurity-blog/the-future-use-cases-of-blockchain-for-cybersecurity>
- <https://onlinedegrees.sandiego.edu/threat-or-opportunity-big-data-and-cyber-security/>
- <https://www.cloudflare.com/en-in/learning/security/glossary/what-is-zero-trust/>
- <https://www.analyticsinsight.net/top-100-cybersecurity-startups-to-look-out-for-in-2021/>
- <https://www.softwaretestinghelp.com/best-cyber-security-companies/>
- <https://www.rapid7.com/fundamentals/types-of-attacks/>
- <https://www.indianext.co.in/top-10-ai-powered-cybersecurity-companies-to-opt-for-in-2023/>
- <https://www.softwaretestinghelp.com/best-cyber-security-companies/>
- <https://startuptalky.com/cybersecurity-startups-india/>
- <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers>

Posted Date: October, 2023

AUTHORS

Mr. Feroz Desai

Ms. P. Prema Latha

TAGS:

COMPUTER SCIENCE

ELECTRONICS

Services

Landscape Search

Technology Alerts

Non-Patent Literature Search

Patentability Search


[Case Studies](#)

[Knowledge Center](#)

GET THE BROCHURE  [Download the pdf file of latest update for this service.](#)

Need Help ?

Please feel free to contact us. We will get back to you within 1-2 business days. Or just call us now

 +1-281-394-4985

 info@patent-art.com

[Contact Us →](#)

SciTech Patent Art

SciTech Patent Art is a big data analytics firm specializing in technology research and analytics. We use innovative AI tools and techniques such as deep web search, and other big data analytics to extract insights from patent and scientific literature, product labels, company websites and other types of information.

Address

🏠 SciTech Patent Art Services (P) Ltd.
📍 Plot. No. 17 & 22, TSIIIC Tech Park,
Road No.12, IDA Nacharam,
Hyderabad – 500 076,
Telangana, India.

☎ +91 9030 09 6188

☎ +91.40.27156181 / 27156182

📞 +91.40.27156184

✉ info@patent-art.com

Quick Links

[Leadership Team](#)

[Services & Capabilities](#)

[Case Studies](#)

[Knowledge Center](#)

Contact Us