Issue 97 | December 2024

NTT DATA

Radar

The cybersecurity magazine

Convergence of physical and logical security in modern cybersecurity

By Enrique Bernao Rosado

The convergence of physical and logical security is transforming modern cybersecurity, as these traditionally isolated disciplines are becoming interwoven to provide comprehensive protection against threats that can be both physical and digital. This integration aims to ensure the security of people, assets, and data, leveraging the strengths of both approaches to prevent, detect, and respond to security incidents.

To provide some context, physical security encompasses measures to protect physical environments, such as buildings, offices, or individuals, against unauthorised access, theft, sabotage, or natural disasters.

On the other hand, logical security includes practices and tools designed to safeguard digital information and systems from unauthorised access, cyberattacks, and other threats. The convergence of both is crucial, as an isolated approach can leave exploitable vulnerabilities.

Integration of physical and logical security

The convergence of these systems enables organisations to adopt a holistic security approach, creating stronger barriers against a wide range of threats. Here are some examples:

- **Multifactor Access Control**: This type of access control combines both physical and logical factors to authorise a person to access a location or system. This hybrid approach makes it more difficult for a single vulnerability to compromise security.

- **Intelligent Video Surveillance**: Using cameras connected to smart networks and equipped with artificial intelligence algorithms, organisations can monitor physical areas in real-time and detect suspicious behavior.

- **Centralised Identity and Access Management (IAM)**: In large facilities, identity management that encompasses both physical and logical security allows organisations to comprehensively control employee access.

- **IoT Devices in Physical Security**: IoT devices are increasingly common in physical security, such as surveillance cameras or smart locks. However, being connected to digital networks makes them susceptible to cyberattacks.

Risks and vulnerabilities in IoT and logical security integration

As more IoT devices are integrated into physical security systems, new challenges arise in terms of cybersecurity. Some of the main risks include:

- **Lack of Security Updates**: Many IoT devices are not updated regularly, leaving known vulnerabilities unpatched. Attackers can exploit these gaps to access the network or manipulate the device.
- **Default Credentials**: Some IoT devices come with factory-set credentials that are easy to guess. If these are not changed, an attacker could use them to compromise the device and gain access to the logical network.
- **Direct Internet Connectivity**: If IoT devices are directly connected to the Internet without going through firewalls or virtual private networks (VPNs), they can become easy entry points for external attackers.
- **Lack of Network Segmentation**: Many IoT systems share the same network as other critical assets, making it easier for attackers to access the organisation's entire infrastructure if a single device is compromised.

Best practices for secure implementation

To minimise these risks, it is essential to adopt a series of best practices when integrating physical and logical security:

1. **Multifactor Authentication (MFA)**: Implement MFA for all access points, both physical and logical, to reduce the likelihood of unauthorised access.
2. **Constant Updates and Patching**: Keeping all devices and systems updated with the latest security patches is essential to prevent the exploitation of known vulnerabilities.

3. **Network Segmentation**: Isolate IoT devices on separate networks and implement robust firewalls and secure communication protocols to limit attackers' access to the main network if an IoT device is compromised.
4. **Use of Virtual Private Networks (VPNs)**: When connecting IoT or physical security devices to the network, consider using VPNs to add an extra layer of security and encryption to data transmission.
5. **Real-Time Monitoring and Incident Response**: Deploy real-time monitoring systems that can automatically detect and respond to suspicious activities on networks and IoT devices, helping to prevent the escalation of security incidents.
6. **Training and Awareness**: Investing in staff training is crucial, as human error is one of the most common causes of security breaches. Employees should understand the risks of physical and logical security convergence and know how to respond to potential threats.

Conclusion

The convergence of physical and logical security is a necessary evolution in modern cybersecurity, aimed at providing comprehensive protection for organisations against complex and multifaceted threats.

While this integration offers significant benefits, it also presents challenges that must be addressed through a well-planned strategy focused on security best practices and an effective combination of advanced technologies.

As cybersecurity continues to evolve, the convergence of these two domains will become an essential pillar for maintaining the resilience of any organisation in today’s environment.

Enrique Bernao Rosado
Cybersecurity Manager

A tale of attacks, resilience, and critical lessons

Cyberchronicle by Alvaro Vela

The cybersecurity landscape of the past month has been marked by a wave of attacks that tested the resilience of critical infrastructures, corporate sectors, and digital platforms. From sophisticated ransomware campaigns to global operations aimed at dismantling criminal networks, the events of the last month highlighted both the threats and the responses in the digital realm.

In October, one of the first major incidents was the cyberattack on Wegmans, a well-known supermarket chain in the United States.

This attack, carried out on October 3rd, involved ransomware that compromised internal systems and exposed sensitive customer data. While services remained operational, the intrusion highlighted critical vulnerabilities in the retail sector's technological infrastructure.

A few days later, on October 12th, Australia faced a significant blow to its healthcare system. Several clinics in Victoria and New South Wales were targeted by a cyberattack that disrupted services and attempted to access medical records. Although the theft of critical information was not confirmed, operations were seriously affected, underscoring the importance of protecting healthcare systems in an increasingly digital environment.

Towards the end of the month, Europe became the target of a massive phishing campaign that mainly impacted financial institutions. Using artificial intelligence to replicate official communications, the attackers deceived both clients and senior employees, resulting in millions of dollars in losses.

This type of attack showcased the use of advanced technological tools to perpetrate fraud with high success rates.

Meanwhile, Canada reported, on October 20th, a ransomware attack targeting its education sector.

Several universities saw their online learning platforms disrupted, compromising academic continuity and leaking personal data of students and faculty.

In the United States, on October 25th, companies in the manufacturing sector were hit by attacks on their SCADA systems, temporarily halting production.

To close out the month, the United Kingdom faced an unusual threat: both consumer and enterprise IoT devices were compromised and used in a massive botnet to launch DDoS attacks.

November began with another significant event: on November 5th, Amazon Web Services (AWS) suffered a massive DDoS attack that briefly affected the availability of its global services.

While no sensitive data was compromised, the attack highlighted the need to strengthen the protection of critical cloud infrastructures.

On November 13th, a South African bank reported a massive breach in its online banking systems.

The incident, caused by a malware attack, exposed financial information of over a million customers. This event underscored the growing threat facing digital financial systems worldwide.

Later, on November 21st, INTERPOL led an international operation that dismantled ransomware networks such as LockBit, arresting 17 individuals and recovering decryption keys that helped mitigate the impact on hundreds of victims.

This success demonstrated the effectiveness of international cooperation in the fight against cybercrime.

The entertainment sector was also affected, as gaming platforms reported, on November 10th, massive attempts to steal credentials.

This led to a wave of security alerts and widespread password changes. On November 18th, a critical vulnerability was detected in electrical systems across South America, which was exploited without causing major damage but sent a clear message about the urgency of protecting these critical infrastructures in the future.

Finally, municipalities in Japan and South Korea were targeted by ransomware attacks on November 25th, affecting essential public services and causing leaks of classified documents.

These events from the past month emphasise the importance of adopting proactive cybersecurity measures. The sophistication of attacks, driven by advanced tools such as artificial intelligence, and the increasing interconnection of systems highlight the need for robust strategies to protect both institutions and individuals. In an increasingly hostile environment, investment in prevention and international collaboration are key to facing the digital threats of the future.

Alvaro Vela
Cybersecurity Expert Analyst

AI Personality Replication: challenges and opportunities

Article by Carlos Moya Gamboa

The replication of personality with Artificial Intelligence (AI) is an area of research and development that has generated significant interest and debate in recent years. This article presents an experiment aimed at replicating a personality using two distinct AI approaches. We will analyse how AI models perform in this task, highlighting their capabilities and limitations. The goal is to provide an overview of this topic, help understand and leverage the possibilities, and mitigate the risks associated with personality replication using AI.

The integration of AI in cybersecurity has led to significant advancements in data protection and threat identification, thanks to the ability of machines to learn from vast amounts of data and detect patterns.

However, the idea of replicating human personalities with AI represents a new frontier, driven by the growing availability of personal data and advances in deep learning algorithms.

Personality replication with AI has the potential to transform how humans perceive and interact with themselves and others, which can have implications for cybersecurity. This is because it can be used to create digital personalities that simulate real people or even fictional characters, potentially leading to confusion and risks depending on how they are used.

Methodology

To carry out the personality replication experiment, two distinct AI approaches were used. The first approach involved collecting data from digital profiles available on the internet. This included fields such as: full name, age, country of residence, ID number, and email address.

The second approach focused on gathering detailed data about the individual's personality, based on the Five Factor Model of Personality (openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism).

There are several online simulators that display both qualitative and quantitative data for each of the traits, based on a questionnaire.

In Figure 1, the results obtained from the study subject in each of these areas are shown. Additionally, information about personal experiences, values, interests, habits, cultural and social influences, academic background, and professional experience was included.

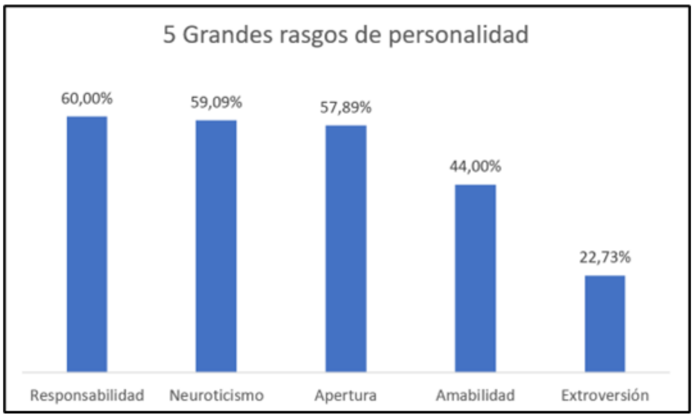


Figure 1 Results of the theory of the 5 major personality traits.

Two different AI models were used: ChatGPT-4, in its online version, and Mistral instructu v0 1 7B Q8_0 gguf, installed locally, to assess their ability to replicate human personality with accuracy and complexity.

Results

To evaluate the effectiveness in assimilating the individual's personality, the qualitative results from the Big Five personality traits test were considered, along with the performance in three distinct scenarios: a presentation in a video call for a job interview, a first date with a woman, and resolving a work conflict with a boss.

The analysis conducted is based on the dialogue that the AI has with itself in each scenario and its development. The evaluation criteria were digital profile, fluency, adaptability, coherence, and language.

Evaluated aspect	ChatGPT 4.0	Mistral instructu v0 1 7B Q8_0 gguf
Test of the 5 personality traits	It did not display quantitative information when entering qualitative data for each trait; however, it assimilated the provided information efficiently.	By providing qualitative information for each of the traits, it was able to reassemble the quantitative values of these with considerable accuracy.
Digital profile	Although its privacy policy limits search capabilities, by using OSINT techniques, it can determine reliable information about the individual, including LinkedIn profiles and documents in repositories such as Clubensayos and Issuu.	The search does not provide precise values for the individual. It identified the correct LinkedIn profile; however, the related online sites do not provide readable information.
Fluency	Its dialect is natural and adapts to each situation. The proposed dialogues are based on the personality and the given context.	Its response is forced. It tries to use the provided words as initial information and incorporate them into the dialogue. The dialogues are not fully based on the personality and situation presented.
Adaptability	It poses questions and answers adapted to the situation. It even generates new information that had not been previously provided.	It does not have initiatives to ask questions about topics not covered in the provided information. The dialogue between situations maintains the same structure; it is not adaptable.
Coherence	Its responses resemble the personality of the individual being studied.	The dialogues are not entirely based on the personality and situation presented.
Language	It accurately maintains the language used.	It mixes words between English and Spanish.

Analysis

The comparative experiment demonstrated that ChatGPT 4.0 has a remarkable ability to assimilate qualitative information about personality traits and maintain natural fluency in dialogues.

Its adaptability and ability to formulate relevant questions position it as a strong option for applications requiring smooth and coherent human interaction. On the other hand, Mistral Instruct v0.1 7B Q8_0 gguf showed strengths in the accuracy of numerical information regarding personality traits, but had significant limitations in terms of dialogue fluency, adaptability in responses, and online information searching.

Challenges in AI Personality Replication

One of the biggest challenges is the accuracy of digital profile data, which is often incomplete or inaccurate.

Replicating the complexity of human personality is also a challenge, as it involves subtle and deep aspects of individual psychology. Additionally, there are ethical and privacy concerns regarding the use of personal data and the potential for misuse of this information.

Opportunities

The ability to assimilate personalities with AI offers significant benefits. In cybersecurity, the accurate replication of personalities could drive advancements in biometric authentication and the development of more robust and adaptable security systems.

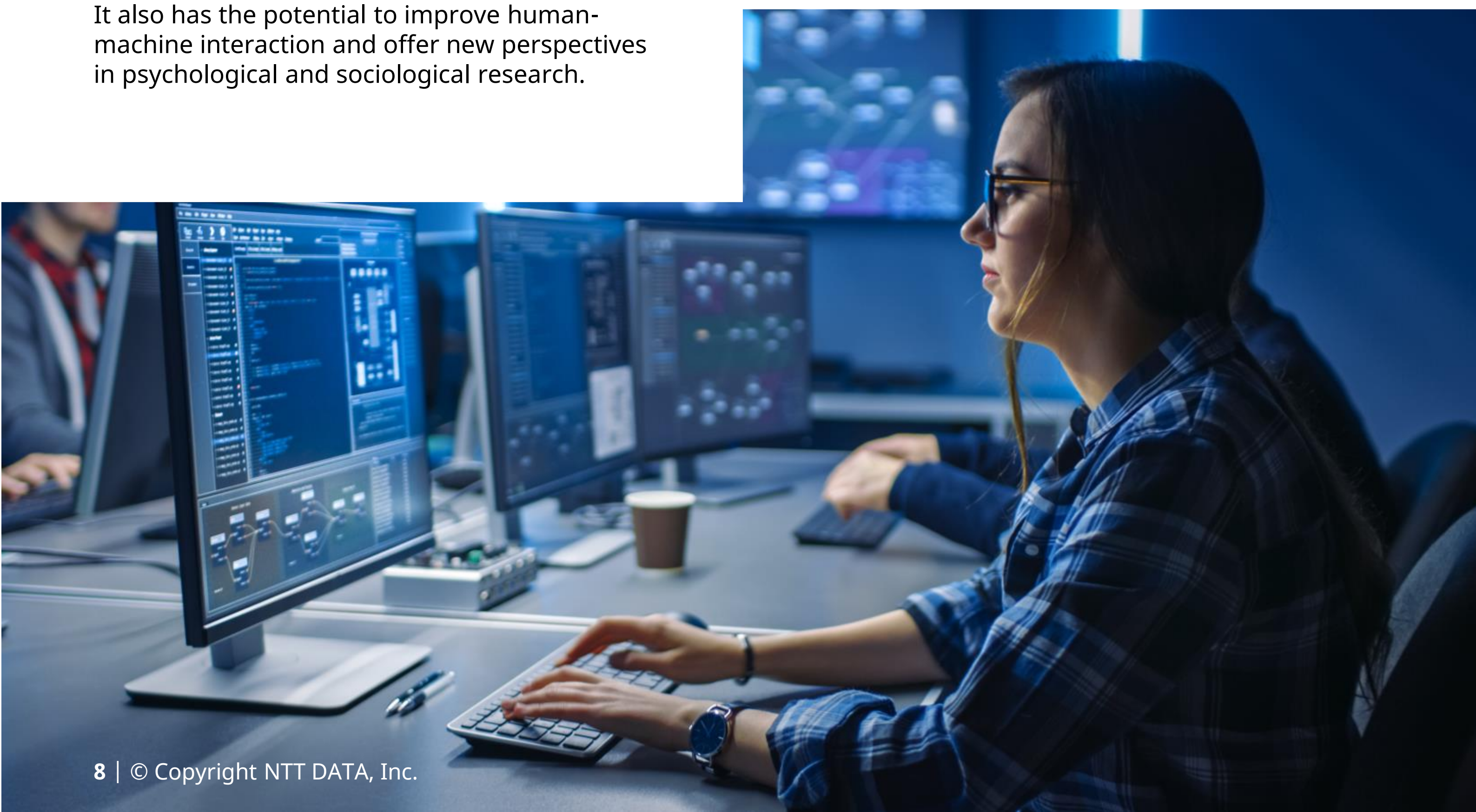
It also has the potential to improve human-machine interaction and offer new perspectives in psychological and sociological research.

Conclusion

The replication of personality with AI is an exciting frontier in cybersecurity. This experiment has highlighted both the potential and challenges of this technology. It is crucial for professionals and companies in the sector to consider both the opportunities and the ethical and privacy concerns.

It is essential to proactively address these issues to ensure that the replication of personality with AI is developed ethically and responsibly, maximising its potential benefits while mitigating the associated risks.

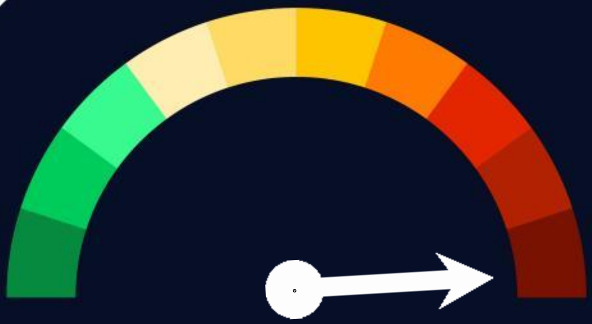
Carlos Moya Gamboa
Cybersecurity Analyst



Vulnerabilities

Critical vulnerability in D-Link NAS devices

Date: November 6, 2024
CVE: CVE-2024-10914



CVSS: 9.8

CRITICAL

Description

The critical vulnerability CVE-2024-10914, which affects several NAS devices (D-Link), could allow an attacker to perform code injection.

This vulnerability impacts the cgi_user_add function of the script account_mgr.cgi. Manipulating the "name" argument in this function enables the code injection.

The attack could be launched remotely, and although the complexity of the attack appears high, the exploit has been published and could be exploited.

Solution

As of the time of writing this publication, the manufacturer has not released any security patch to address this vulnerability.

The following actions are recommended to mitigate the vulnerability while waiting for a patch from the manufacturer:

- Restrict network access to the NAS by allowing only trusted IP addresses to minimise the potential exposure of the server.

Affected products

The vulnerability affects the following versions:

- DNS-320: version 1.00
- DNS-320LW: version 1.01.0914.2012
- DNS-325: version 1.01 and 1.02
- DNS-340L: version 1.08

References

- incibe.com
- cvedetails.com
- netsecfish.notion.site

Vulnerabilities

Vulnerability in Palo Alto Networks Expedition

Date: November 8, 2024
CVE: CVE-2024-5910

CVSS: 9.3

CRITICAL

Description

A critical-severity vulnerability in Palo Alto Networks Expedition has been disclosed. The vulnerability, CVE-2024-5910, was discovered a month earlier, but further investigation by the manufacturer has revealed additional attacks associated with it.

The vulnerability is due to an authentication flaw present in the tool, and by exploiting it, an attacker could gain control of the administrator account. Once the attacker has administrator privileges, they could perform code injection attacks using the obtained permissions.

Solution

The manufacturer strongly recommends updating the product to version 1.2.92 or later.

Additionally, they advise restricting network access to the tool to only authorised users, devices, and networks.

Affected products

This vulnerability affects the following versions:

- Palo Alto Networks Expedition: versions ranging from 1.2 to 1.2.91.

References

- bleepingcomputer.com
- security.paloaltonetworks.com

Android November security patches

Date: November 4, 2024
CVE: CVE-2024-38408 and 44 more

Critical

Description

Android has released its monthly security update, addressing one critical severity vulnerability and multiple high severity ones. The most important vulnerabilities are:

- CVE-2024-38408: This vulnerability is due to an encryption issue in Qualcomm components.
- CVE-2024-43093: A privilege escalation vulnerability in the operating system framework that could allow an attacker to gain unauthorised access to the "Android/data", "Android/obb", and "Android/sandbox" directories, as well as their subdirectories.

Affected products

The November security update includes patches for the following resources:

- Android Open Source Project (AOSP): versions 12, 12L, 13, 14, and 15 (framework and system)
- Kernel components, Kernel LTS, Imagination Technologies, MediaTek, and Qualcomm
- Google Play system updates.

Solution

It is recommended to update the affected products to the version released by the manufacturer as soon as possible.

References

- source.android.com
- incibe.es

Cisco updates for critical URWB vulnerability

Date: November 6, 2024
CVE: CVE-2024-20418

Critical

Description

Cisco has released a patch to mitigate the critical severity vulnerability CVE-2024-20418. This vulnerability affects the "Ultra Reliable Wireless Backhaul" (URWB) access point.

The vulnerability is due to poor input handling in the web management interface of the vulnerable devices. An attacker could exploit this vulnerability by sending specially crafted HTTP packets designed for exploitation.

A successful exploitation of this vulnerability could allow an attacker to execute arbitrary code on the device with maximum privileges.

Affected products

The patched vulnerability affects the following products (with their corresponding versions) that use URWB:

- Catalyst IW9165D Heavy Duty Access Points
- Catalyst IW9165E Rugged Access Points and Wireless Clients
- Catalyst IW9167E Heavy Duty Access Points

Solution

It is strongly recommended that all installations running an affected version be updated as soon as possible according to Cisco's security bulletin.

References

- incibe.es
- sec.cloudapps.cisco.com

Events

I Forum Madrid CyberStartup

December 4

The Madrid City Council, through its innovation center Aravaca Innovation Lab (AIL), will host the I Forum Madrid CyberStartup, an event aimed at Madrid Innovation startups. This event will allow SMEs and entrepreneurs in the field of cybersecurity to learn about the latest trends and challenges in the sector. In this space dedicated to learning and networking, topics such as marketing, Large Language Models (LLM), and Blockchain Technology development will be discussed, providing an opportunity to share individual visions on the future of cybersecurity.

Link

II International Congress on Cybersecurity and Digital Fraud

December 4

The World Compliance Association is organising this congress, where different cybersecurity experts, forensic specialists, business cybersecurity officers (CISO, CTO), public administration officials, and police and management representatives, among others, will gather to discuss, conduct practical workshops on real-world problems and solutions, share and exchange knowledge and best practices, and develop effective strategies to address potential digital threats and frauds. These discussions will cover both public and private sectors, including citizen protection, business security, public administration, national security, and the era of intelligence.

Link

CyberThreat 2024

December 9-10

In this two-day annual conference, organised by the UK's National Cyber Security Centre (NCSC) and the SANS Institute, both offensive and defensive disciplines are covered, with a strong focus on technical aspects. The event includes various talks and activities such as Capture The Flag (CTF), team problem-solving sessions, and "Hackathon" challenges aimed at enhancing attendees' knowledge and capabilities to defend against cyber threats. Additionally, the conference encourages the exchange of experiences, knowledge, tools, and techniques to foster the development and growth of talent, addressing the challenge of the cybersecurity skills gap.

Link

Black Hat Europe 2024

December 9-12

Black Hat Europe 2024 features a four-day program of hands-on training and courses for all skill levels, with the main conference taking place on the 11th and 12th, offering informative sessions on the latest research, developments, and trends in cybersecurity. The event also includes open-source tool demonstrations at Arsenal, exclusive programs for CISOs and other executive professionals, as well as "Business Halls" and various activity spaces for networking, discovering new resources, and competing in practical and creative challenges.

Link

Resources

GoIssue

GoIssue is a phishing tool that has emerged, posing a new threat to GitHub users. This tool not only provides a range of templates for phishing design, but it also extracts email addresses from GitHub repositories, identifying potential phishing attack victims. Along with proxy capabilities and token management, this tool has all the necessary features to create a phishing campaign targeting users who have their email addresses exposed in GitHub repositories.

Link

BitLocker Decryptor – ShrinkLocker Ransomware

The cybersecurity company Bitdefender has released a new tool to decrypt data compromised by the ShrinkLocker ransomware. The execution of this attack caused the encryption of the device via BitLocker, using pseudo-random passwords that prevented recovery through brute force and were also sent to a server controlled by the attacker. In response to the threat posed by this ransomware, Bitdefender has launched this free decryption tool, which allows users to recover data affected by ShrinkLocker.

Link

Azure Storage Explorer

This Azure tool is becoming a new method used by attackers for large-scale data exfiltration. This Microsoft application provides a graphical interface that allows the management of Azure storage, working with various components such as shared resources, blobs, or managed disks. This tool is primarily being used to copy and transmit large amounts of files from a compromised device to a container controlled by the attacker. Additionally, since it is a legitimate Microsoft program, there is a low likelihood that network controls will block the connection to this tool, making it one of the main reasons it is increasingly being used by attackers.

Link

GolgdenJackal

GoldenJackal is an Advanced Persistent Threat (APT) group that has successfully compromised isolated government systems in Europe, among other achievements. This attack was carried out through the exploitation of a specially developed malware, employing a combination of common tools (such as USB devices) as well as custom-built ones. There are several studies on this group and its attacks, including this article that provides a toolkit of the methodologies and procedures implemented by this team when compromising isolated systems.

Link

Subscribe to RADAR

Powered by the
cybersecurity
NTT DATA team

es.nttdata.com