# NCC Group Research Report 2022 & 2023

Matt Lewis, Global Head of Research &
Ristin Rivera, Research Program Coordinator

research.nccgroup.com

Our 2022-2023 Research Report is also available in downloadable PDF

nccgroup

# Table of Contents

# Executive Summary: Research at NCC Group (2022 & 2023)

**Over the past two years, our global cybersecurity research has been characterized by unparalleled depth, diversity, and dedication to safeguarding the digital realm. The highlights of our work not only signify our commitment to pushing the boundaries of cybersecurity research but also underscore the tangible impacts and positive change we bring to the technological landscape. This report is a summary of our public-facing security research findings from researchers at NCC Group between January 2022 and December 2023.**


With the release of 18 public reports and presenting our work at over 32 international conferences and seminars, encompassing a variety of technology and cryptographic implementations, we have demonstrated our capacity to scrutinize and enhance key security functions. Notably, our collaborations with tech giants such as Google, Amazon Web Services (AWS), and Kubernetes underscore our pivotal role in fortifying the digital ecosystems of industry leaders.

Commercially, 2022 and 2023 saw us deliver over $3million in revenue in collaborative research engagement across various technologies and many sectors, increasingly across Artificial Intelligence (AI) and AI-based systems.

In our bid to democratize cybersecurity knowledge, we have released 21 open-source security tools and repositories. These invaluable tools have catalyzed efficiency gains across multiple domains of cybersecurity.

Our research has positioned us at the forefront of evolving cryptographic paradigms. With significant work in Post-Quantum Cryptography, Elliptic Curve Cryptography, and Blockchain security, we remain key players in shaping the future of digital privacy and security.

The meteoric rise of AI/ML applications has been matched by our intense focus on understanding their security dynamics. Our research in this arena has grown exponentially since 2022, providing critical insights into the strengths and vulnerabilities of these transformative technologies.

Modern cloud environments, coupled with rapid shifts in software development and deployment, have necessitated deep dives into their security mechanisms. Our outputs in this domain have been instrumental in pioneering robust cyber defense tactics for contemporary digital infrastructures. Our exhaustive studies into hardware vulnerabilities and Operating System security have set benchmarks in comprehending and countering potential threats.

The external presentation of our research, particularly by our Exploit Development Group (EDG), has won us accolades, most notably a third-place finish at the 2022 Pwn2Own Toronto competition. EDG's work on exploiting consumer routers and enterprise printers has been groundbreaking. Ken Gannon and Ilyes Beghdadi successfully exploited the Xiaomi 13 Pro smartphone at the 2023 Pwn2Own Toronto competition, demonstrating our continued excellence in mobile security.

Our research has spanned several other pivotal areas including Vulnerability Detection & Management, Reverse Engineering, Modern Networking & Security, and Secure Programming & Development. Unearthing over 69 security vulnerabilities across third party products, we've reinforced our commitment to digital safety through responsible and coordinated vulnerability disclosure. Each discovery, while highlighting potential threats, also underscores our unwavering dedication to proactively fortifying global digital infrastructures.

In conclusion, our journey through 2022 and 2023 has been marked by rigorous research, collaboration, and an unwavering commitment to excellence. As we continue to gain intelligence, insight and to innovate, our role in shaping a secure digital future remains paramount.

# Message from Global Head of Research, Matt Lewis

**The big cybersecurity challenges for the next 5-10 years relate to ever-evolving technology and threat landscapes, and the need for agility to keep pace in line with these evolutions against the backdrop of a volatile geopolitical landscape. Research has never been more important to help us in our endeavor to achieve security and resilience in these times.**

On a technology level, legacy IT systems and maintenance of software patches remain a key challenge. Organizations are currently in mixed states of security posture in terms of legacy equipment and cloud migration and adoption. Many of the security promises of cloud haven't been met (or understood), meaning that even cloud systems can and do suffer from legacy issues such as out of support, potentially vulnerable components. Advanced Persistent Threat (APT) intrusions and Ransomware outbreaks routinely exploit legacy or unpatched systems for their gain, thus there is still much to do in terms of mitigating risk around legacy, noting that the new technologies of today, will also become legacy in 5 or 10 years' time, therein establishing legacy IT as a permanent challenge for cybersecurity.

While APTs are a huge threat to organizations and the global economy, the reality is that in terms of impact, ransomware is a much more pressing and damaging threat. A key challenge here is how to ensure organizations remain resilient in the face of a ransomware outbreak, since even a fully patched, cyber mature organization could be subject to a sophisticated ransomware attack exploiting a 0-day vulnerability.

AI and Machine Learning is already proving a challenge in terms of the requirement to gain a robust understanding of their relative opportunities and threats. The sudden accessibility of performant Large Language Models (LLMs) like ChatGPT in 2022 took most sectors, cybersecurity included, by surprise. There are already several potential negative impacts of LLMs in terms of cyber security, the security of the models themselves in how they are created and understanding how and why they produce their outputs. There is also concern for how and where and by whom LLMs are used – perhaps in generating source code for malware, or attack methodologies that make it easier for less technical individuals to perform offensive cyber activities. There are also big challenges in the realm of misinformation and, with related commoditized capabilities like Deepfakes, the emerging threat of Identity Compromise to support fraudulent activities – certainly, the industry is already seeing a natural evolution and sophistication of misinformation and targeted phishing campaigns leveraging these capabilities.

The growing use of AI as a security control also presents a huge challenge – the efficacy of such solutions demands robust testing, evaluation and assurance, lest we become too trusting of automated decision making in security governance that we believe to be optimal but in fact may be silently rendering our systems more vulnerable.

It is possible we will see Quantum Supremacy in our lifetime, meaning there is a burgeoning challenge in preparing businesses for Post-Quantum Cryptography (PQC). While the preparation requirements and PQC algorithms are broadly understood, ensuring a worldwide migration to robust PQC presents a challenging undertaking.

Related to quantum is the need to manage the threat model of classical computing integration with quantum components. The traditional vulnerabilities in classical computing will inevitably present potential for adversary exploitation to gain unauthorized access to quantum computing resources. There are also challenges in needing to understand and assure applications of quantum computing to cryptographic processes, namely Quantum Random Number Generation (QRNG) for seeding cryptographic material, and Quantum Key Distribution (QKD) for managing cryptographic keys and exchange.

Despite their challenges, the technologies discussed above can be seen as the foundations and backbone for the broader concept of the connected society or connected world. Exponentially, this concept increases the attack surface of global economies, as seen through Internet of Things (IoT), Smart Cities and Connected Places, Connected and Autonomous Vehicles to name but a few. These application areas also move us rapidly into the cyber-physical domain, meaning the cyber challenges here are not only impacting on a security level, but also safety, whereby the effects of compromise of some systems could lead to environmental impact, physical harm or worst-case loss of life.

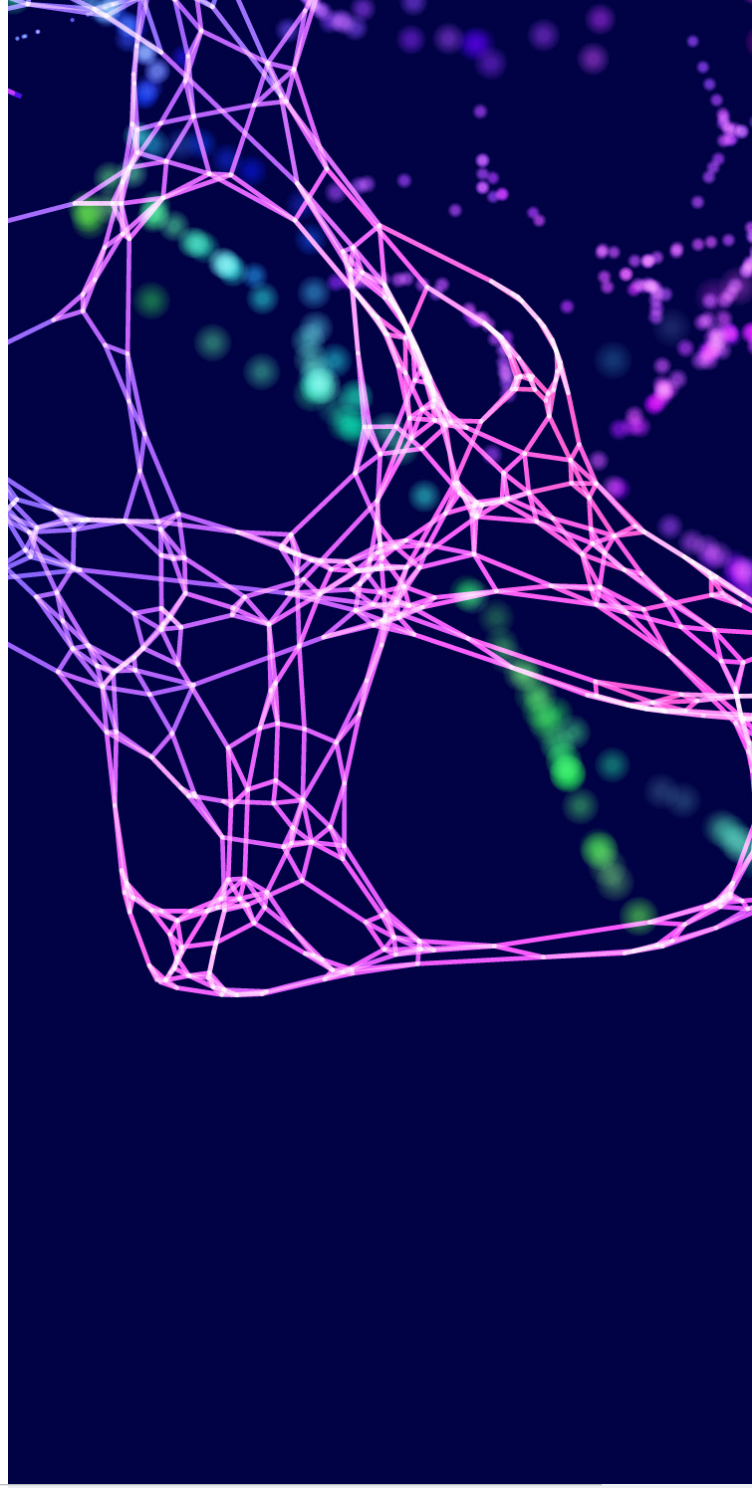
Fueled by the COVID-19 pandemic push for increased home working, we have inadvertently lost the concept of the ‘network perimeter’, but also legitimized this through concepts such as Zero Trust networks. This brings huge challenges around the need to authenticate and authorize directly connected Internet users and machines in trusted, secure and reliable ways.

Supply chain and sovereignty also pose challenges in the present and near future. Lack of trust in supply chains and countries of manufacture has led to a strategic goal for many developed economies to increase their sovereign capabilities and therefore reduce reliance on global manufacturing hubs. Challenges here mostly relate to funding and skillsets required to demonstrate that countries have their own secure capabilities that can deliver in this space.

There is also a broader research challenge relating to horizon scanning and knowing how and where to prioritize security advice and guidance on technologies in terms of their likely adoption. Examples we can expect to see in the next 10 years include Brain Computer Interfaces (BCIs), the Metaverse and its associated VR/AR technologies, increased space-based telecoms, neuromorphic computing and synthetic biology to name but a few – understanding the security capabilities and issues with these technologies will require vast amounts of research.

Finally, yet crucially, there is a fundamental research challenge around energy use in the face of an energy crisis and climate change. There are estimates that 21% of the world’s overall energy usage by 2030 will be computing power alone, yet technologies in AI, Cloud and Quantum are inherently power-hungry. We therefore need to be incredibly mindful of, and proactive in the development of secure, power-efficient and sustainable technical solutions for the technologies and systems that we will create and use over the coming decade.

Continuously evolving technology and threat landscapes is why research is at the heart of what we do at NCC Group. Our global team of researchers routinely tackle many of these topics and themes to understand risk and remediation across all technologies in all sectors. This report sets out just some of the research insights from our broad research program over the past couple of years. The research doesn’t stop however, and we’re already embracing the research challenges of 2024 and beyond...



# Foreword from Research Coordinator, Ristin Rivera

In our increasingly digital world, the first indication of a security breach often emerges only after the damage has been done, leaving individuals and organizations to grapple with the aftermath. For the average person, without a security team to monitor their network and devices, the assumption is often made that regulatory safeguards would prevent the release of vulnerable products into the market. This assumption, however, can prove to be a significant risk.

Take for example the pervasive world of white-labelled products, particularly in everyday technology. As shown from many of our research outputs from the past couple of years, these cost-effective, ubiquitous products are not always synonymous with security. Repeatedly, our research on white-labelled products, like home routers and IoT devices, reveals that they have little to no security assurance or onward maintenance by manufacturers. They never receive crucial firmware updates or security patches, thus rendering them vulnerable and exposing users and consumers to a myriad of risks. The rise of Bluetooth technology in security-critical applications, such as car key unlocking systems, further highlights this issue which doesn't necessarily correlate with 'cheap' products and services alone - despite Bluetooth's own guidance on the limitations of its security features, the trend persists, as seen through our research demonstrating remote keyless attacks to gain entry to, and drive off with Tesla motorcars (a premium product) as just one example.

This unseen vulnerability represents the Achilles heel of cybersecurity. Proactive security measures, regular check-ups, and a comprehensive understanding of the limitations of our technology through continued research and innovation are not merely best practices; they are essential pillars of a robust cybersecurity strategy.

# AI & Machine Learning

In the dynamic landscape of cybersecurity, the domain of Artificial Intelligence and Machine Learning (AI/ML) security research has emerged as a paramount focal point. As AI/ML systems become deeply integrated into the very fabric of our society, influencing sectors from healthcare to finance, and from transportation to communication, their security and safety cannot be understated. Ensuring the robustness of these systems is not merely a technical necessity but a societal imperative. With AI playing an ever-impacting role in decision-making processes, personal interactions, and infrastructure, researching its security contours is critical to safeguarding the trust and wellbeing of individuals and institutions that increasingly rely on it. Unsurprisingly, AI/ML research at NCC Group has grown exponentially since 2022, as we continue to grasp the security and safety strengths and limitations of these powerful capabilities. Key observations from our AI/ML research since 2022 were:

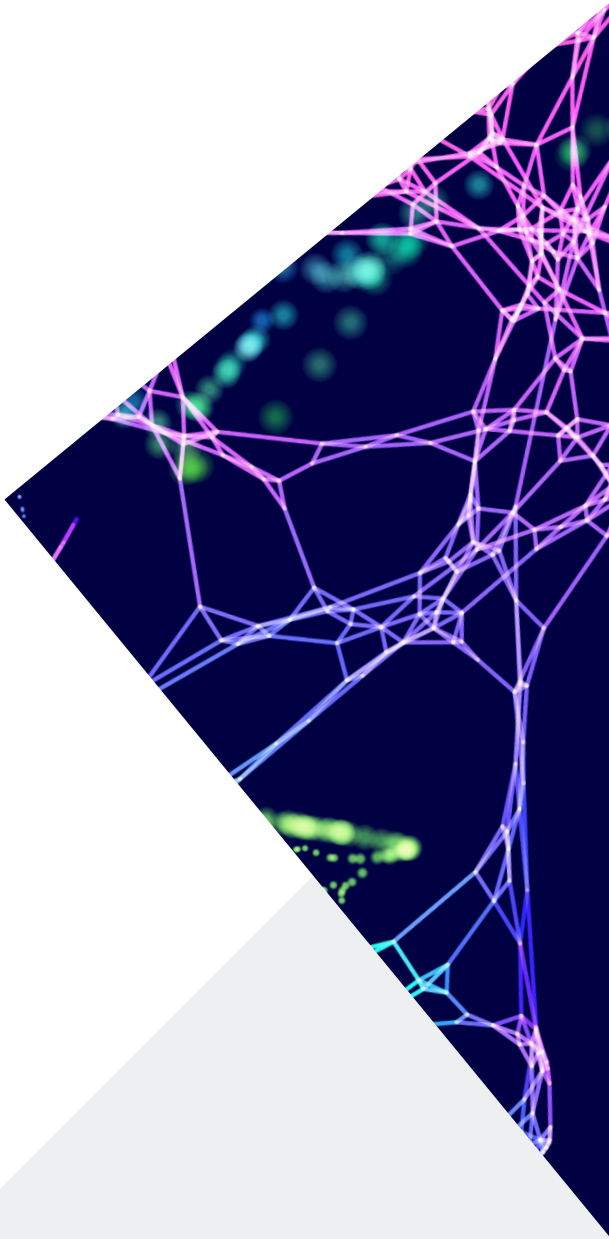
- Potential and Pitfalls of AI/ML: The transformative power of AI and ML in cybersecurity is clear, but so are the associated risks and challenges
- Impersonation and Privacy Concerns: AI's capability to mimic human interactions can lead to serious privacy concerns, especially in community-driven platforms
- ML in Malware Analysis: ML significantly enhances malware detection but is not immune to challenges like adversarial attacks
- Security Implications in ML Systems: Adversarial attacks, data poisoning, and model extraction are major concerns in ML security
- Large Language Models (LLMs): Their power and potential come with challenges around overfitting and data reproduction
- Human Oversight: Despite AI's capabilities, human expertise remains paramount in cybersecurity tasks, from code review to threat detection

### Potential and Pitfalls of AI/ML

Jon Renshaw summarized much of our research in an informative whitepaper, to assist those wishing to better understand how AI applies to cybersecurity. The paper provides high-level summaries of how AI can be used by both cyber professionals and adversaries, the risks AI systems are exposed to, safety, privacy and ethics concerns and how the regulatory landscape is evolving to meet these challenges.

Practical Attacks on Machine Learning Systems: NCC Group's Chief Scientist authored this formative paper which collects a set of notes and research projects conducted by NCC Group on the topic of the security of ML systems. The paper provides industry perspective to the academic community, while collating helpful references for security practitioners, to enable more effective security auditing and security-focused code review of ML systems. Details of specific practical attacks and common security problems are described throughout the paper.

Security Implications in Machine Learning: Chris Anley's blog, "Five Essential Machine Learning Security Papers," underscores the security challenges in ML systems as seen through landmark exploitation techniques described across five key academic papers.



Code Review with AI and ML: We wrote articles discussing the intersection of code review and ML. From using Semgrep with Jupyter Notebook files by Jose Selvi to Chris Anley's caution against using ChatGPT for security code reviews, there is a clear acknowledgment of ML's growing influence in this domain. However, there is also a recognition of its limitations, emphasizing human expertise's continued relevance.

> *Don't use ChatGPT for security code review. It's not meant to be used that way, it doesn't really work (although you might be fooled into thinking it does), and there are some other major problems that make it impractical. Also, both the CEO of OpenAI and ChatGPT itself say that you shouldn't.* ***- Chris Anley, NCC Group Chief Scientist***

Intelligent Web Crawling with ML: Project Bishop, performed by Thomas Atkinson and Jose Selvi, was a continuation of Project Ava and explored the use of ML for intelligent web crawling. It emphasized the power and potential of ML in enhancing web application security testing tasks.

> *Generative AI is stealing the spotlight at the moment but smaller, specialized AI/ML models that can be run locally are also becoming usefully powerful to run on accessible consumer grade hardware. In the coming years we should expect both attacker and defender tooling to increasingly make use of these smaller, localized models.* ***- Thomas Atkinson, Managing Security Consultant***

Eric Schorn provided great insight across a range of ML topics in a blog series that will continue into 2024 across 10 eventual lessons:

- Machine Learning 101: The Integrity of Image (Mis)Classification: This blog highlights various security-related weaknesses in ML systems. Topics range from the brittleness of image classification models to attacking facial authentication systems with poisoned data, emphasizing the criticality of mitigating these weaknesses.
- Machine Learning 102: Attacking Facial Authentication with Poisoned Data: This blog post demonstrates exactly how a data poisoning attack might work to insert a backdoor into a facial authentication system.
- Machine Learning 103: Exploring LLM Code Generation: This executable blog post explores code generation from a 16 billion-parameter large language model (LLM).
- Machine Learning 104: Breaking AES with Power Side-Channels: In this post, Eric discusses how deep ML techniques can be used in cryptography, revealing potential vulnerabilities in systems hitherto considered impregnable.

## ML in Malware Analysis

Machine Learning for Malware Analysis: Matt Lewis' work with University College London (UCL) on "Machine Learning for Static Analysis of Malware: Expansion of Research Scope" showed the utility of ML in enhancing static analysis of malware. By leveraging ML, there is potentially improved efficiency in processing data and recognizing malicious patterns, thus offering better detection rates than traditional methods. However, adversarial attacks present a potential challenge to these methods, underscoring the importance of robust defenses.

## Impersonation & Privacy Concerns

AI-generated Impersonation: In the article "Impersonating Gamers with GPT-2", David Brauchler deep dived into the use of OpenAI's GPT-2 model to mimic gamers' conversations. The key theme here was the potential security and privacy risks that come with AI-generated content, especially within online communities like gaming. The research effectively demonstrated GPT-2's ability to create a convincing imitation of user interactions, emphasizing the urgent need for countermeasures against AI-driven impersonation attacks.

## Large Language Models (LLMs)

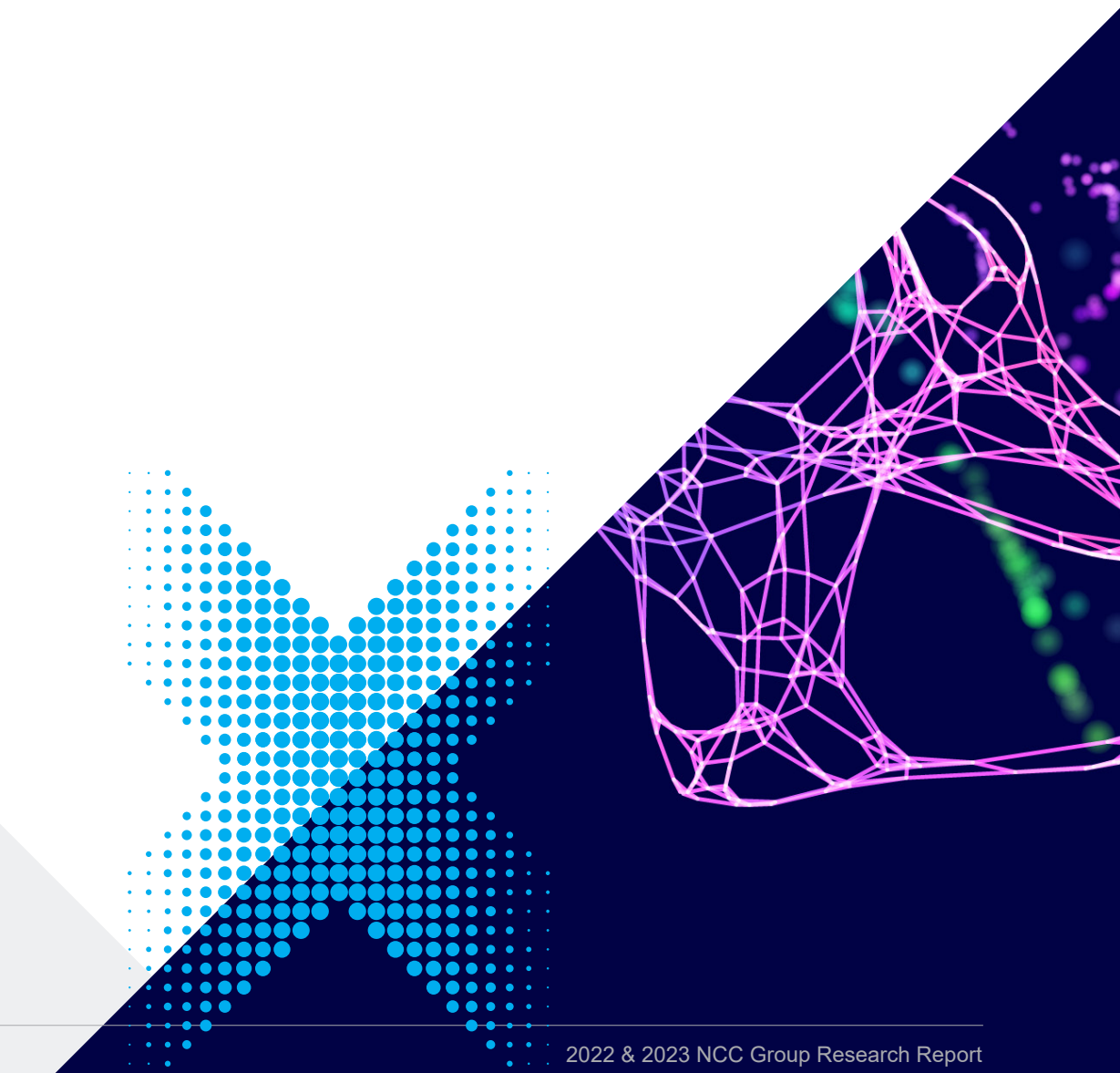
Prompt Injection Vulnerabilities: "Exploring Prompt Injection Attacks" by Jose Selvi delved into the vulnerabilities in terminal sessions, where attackers can manipulate command prompts to inject malicious LLM behaviors.

> *Treat the output of your Large Language Model (LLM) as untrusted data within your threat model. While AI providers implement safeguards against threats such as Prompt Injection, attackers can still manipulate inputs to generate unexpected outputs. These outputs may include payloads that exploit vulnerabilities in the underlying application or infrastructure.* ***- Jose Selvi, Executive Principal Security Consultant***

Matt Lewis explored the potential data security challenges around LLM prompt security, through an example of how a seemingly innocent set of user prompts could potentially lead to unwanted profiling of that user.

Large Language Models (LLMs) and Overfitting: Several articles, such as "Exploring LLM Code Generation" and "Exploring Overfitting Risks in Large Language Models" by Jose Selvi, address the potential and pitfalls of LLMs. Concerns like overfitting, data inference, and the reproduction of copyrighted content underline the caution required in leveraging these models.

> *AI security is a pressing concern in security research. As artificial intelligence systems become increasingly integrated into our lives, safeguarding them against malicious attacks and ensuring their ethical use is paramount. Ongoing research is crucial to stay ahead of emerging threats and develop robust defense mechanisms." -* ***ChatGPT (prompted about its own security)***



# Incident Response & Threat Intelligence Research

Several high-caliber research outputs from our threat intelligence and incident response teams the past two years provide a multi-faceted view of the current threat landscape, from nation-state advanced persistent threats (APTs) to new malware variants and evolving ransomware tactics.

Across this research, several recurring themes and trends emerged:

- Lateral Movement via Remote Desktop Protocol (RDP): Multiple threat actors, including those deploying ShadowPad, LockBit 3.0, Everest, and Black Basta, utilized RDP for lateral movement within a compromised environment
- Use of Legitimate Tools for Malicious Purposes: Tools like ADFind, PowerView, and Cobalt Strike are leveraged by various threat actors for information gathering, command and control, and lateral movement
- Persistent Threats in App Stores: Despite ongoing efforts to secure platforms like the Google Play Store, malicious actors continue to infiltrate it, as seen with SharkBot
- Diverse Initial Access Methods: From exploiting vulnerabilities to leveraging social engineering on platforms like LinkedIn, threat actors employ a range of methods to gain initial access to target environments

> *Cyber threat is a constantly evolving space, presenting unique challenges for organizations aiming to safeguard their digital assets. One of the most effective ways to stay ahead of these threats is through vigilant incident response and in-depth threat intelligence research. These two facets of cybersecurity not only facilitate timely responses to attacks but also offer insights into the tactics, techniques, and procedures (TTPs) of adversaries.-* ***Matt Hull, Global Head of Threat Intelligence***

In summary, these research outputs underscore the need for organizations to continuously adapt and evolve their cyber defenses, given the dynamic nature of threats and the sophisticated tactics employed by adversaries.

### Real-World Compromise & TTPs

2000 Citrix NetScalers backdoored in mass-exploitation campaign: Fox-IT uncovered a large-scale exploitation campaign of Citrix NetScalers in a joint effort with the Dutch Institute of Vulnerability Disclosure (DIVD). An adversary had been identified exploiting in automated fashion, placing webshells on vulnerable NetScalers to gain persistent access. The adversary could execute arbitrary commands with the webshell, even when a NetScaler was patched and/or rebooted. The Dutch Institute of Vulnerability Disclosure notified the victims as identified by Fox-IT. At the time of the exploitation campaign, Fox-IT enumerated 31,127 NetScalers worldwide that were vulnerable to CVE-2023-3519.

> *"In light of several serious FortiGate, Citrix and Cisco vulnerabilities, edge device exploitation is picking up its pace. As your network's first line of defence, visibility on these devices is often scarce and overlooked, making responding to these threats difficult. We believe investing in visibility, such as central logging, patch management and Incident Response readiness will make the difference when it comes to responding to these types of threats. "–* ***Security Research Team, Fox-IT (part of NCC Group)***

ShadowPad Intrusion: William Backhouse, Michael Mullen, and Nikolaos Pantazopoulos provided insights into the TTPs of a Chinese APT leveraging the ShadowPad malware. Initial access was achieved through a vulnerability, with successive backdoors being installed. Tools like ADFind and PowerView were used for information gathering, and ShadowPad was used extensively for lateral movement, command and control, and data exfiltration.

BUMBLEBEE Malicious Loader: This research highlighted BUMBLEBEE, a new loader that incorporates anti-analysis techniques and utilizes Rabbort.DLL for process injection. It can download and execute malicious payloads such as Cobalt Strike beacons.

Post-Conti Data Leaks: Despite the public disclosure of Conti's tools and conversations, Conti operators continued their activities. Techniques observed include the use of Cobalt Strike and different legitimate remote access software for persistence.

Saitama Implant Detection: A novel malware sample named ‘Saitama’ used DNS for C2 communications, making detection challenging. This article outlined the development of a server-side implementation for the implant to aid detection.

Karakurt Extortion Actor: NCC Group’s CIRT discovered indicators of compromise from Karakurt, an extortion-focused threat actor, especially in environments using single factor Fortinet VPN access.

LAPSUS$ TTPs: Incidents involving LAPSUS$ revealed tactics such as scraping corporate SharePoint sites, accessing password managers, and cloning git repositories.

MetaStealer Analysis: MetaStealer emerged as a new information stealer, notable for its reliance on open-source libraries and a range of functionalities including password stealing and keylogging.

Lazarus Initial Access: The Lazarus group’s initial access phase involved impersonating LinkedIn profiles, enticing victims to download malicious documents, and using scheduled tasks for persistence.

Popping Blisters for research: An overview of past payloads and exploring recent developments. Mick Koomen provided an overview of payloads dropped by the Blister loader, based on 137 unpacked samples across an 18-month period.

The Spelling Police: Searching for Malicious HTTP Servers by Identifying Typos in HTTP Responses: Margit Hazenbroek of Fox-IT blogged about identifying servers that host nefarious activities by looking for anomalies in responses of HTTP servers.

SharkBot on Google Play: Our Threat Intelligence team identified and reported instances of the SharkBot Android banking Trojan being distributed through the official Google Play Store.

## Ransomware

LockBit 3.0 Ransomware Attack: Ross Inman explored a LockBit 3.0 ransomware deployment, highlighting initial access via SocGholish, Cobalt Strike for command and control, and the disabling of defensive measures like Windows Defender. Exfiltration occurred through Mega.

Everest Ransomware Group: This article dived into the TTPs of the Everest Ransomware group, noting techniques such as lateral movement via RDP and the use of LSASS and NTDS.dit dumps.

Ransomware Entry Techniques: Michael Mathews delved into common entry methods used by ransomware affiliates, shedding light on the increasing trend of Ransomware as a Service (RaaS).

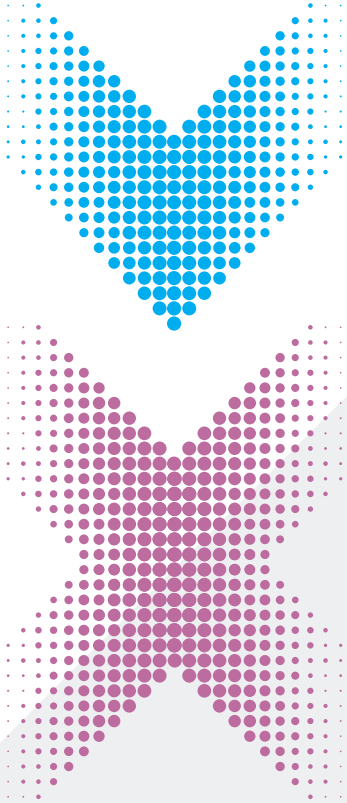
Black Basta Ransomware: Ross Inman and Peter Gurney shed light on the TTPs of the Black Basta ransomware, including lateral movement using Qakbot and the technical breakdown of the ransomware executable.

Unveiling the Dark Side: A Deep Dive into Active Ransomware Families: The CIRT Team look at the return of the BlackCat Ransomware-as-a-Service (RaaS)

D0nut encrypt me, I have a wife and no backups: Ross Inman provided a deep dive into the D0nut extortion group.

Don’t throw a hissy fit; defend against Medusa: Molly Dewis provided a deeper dive into the Medusa ransomware family.

Is this the real life? Is this just fantasy? Caught in a landslide, NoEscape from NCC Group: Alex Jessop delved into a real-world incident response engagement handled by NCC Group’s CIRT, which involved the RaaS known as NoEscape.



# Applied Cryptography

NCC Group's Crypto Services team continued to perform leading research throughout 2022 and 2023. The variety of their rich outputs reflects the ever dynamic and evolving nature of the field of cryptography. Key themes from our crypto research during this period were:

- Post-Quantum Cryptography: The push towards post-quantum cryptography is evident, with discussions on both its challenges and the introduction of new algorithms
- Elliptic Curve Cryptography: A significant portion of our research focused on elliptic curves, highlighting their continued importance in cryptographic systems
- Security Vulnerabilities: From erroneous computations to time-based side-channel attacks, we further explored vulnerabilities in cryptographic implementations and their implications
- Blockchain and Cryptography: Several of our outputs emphasized the relationship between cryptographic principles and blockchain technology

> *Cryptography is a key component of every organization's data security. Cryptography analysis and research is critical to identify impactful cryptography vulnerabilities in today's products and applications. Cryptography Services' research in the ever-changing cryptography landscape ensures that the team continually contributes to the secure design and implementation of cryptography in a wide variety of areas.* ***Javed Samuel, Global VP for Cryptography Services***

## Elliptic Curve Cryptography

Pairing-Based Cryptography: Giacomo Pope detailed pairing-based cryptography, especially the "pairing-friendly" elliptic curves. A key highlight was the estimation of bit security and the advancements in solving the discrete log problem, which has implications on the reported bit-security of several widely used curves.

Elliptic Curve Cryptography: Thomas Pornin's contributions encompassed the domain of practical elliptic curve cryptographic systems. A new pair of elliptic curves, jq255e and jq255s, were proposed as efficient alternatives to existing standard curves.

Giacomo Pope presented on Superspecial Cryptography Computing Isogenies Between Elliptic Products

Thomas Pornin published several papers on Elliptic Curve Cryptography:

- Faster Complete Formulas for the GLS254 Binary Curve
- EcGFp5: a Specialized Elliptic Curve
- Truncated EdDSA/ECDSA Signatures
- Point-Halving and Subgroup Membership in Twisted Edwards Curves
- Efficient and Complete Formulas for Binary Curves
- Optimized Discrete Logarithm Computation for Faster Square Roots in Finite Fields
- Double-Odd Jacobi Quartic and https://doubleodd.group/

## Post-Quantum Cryptography

Post-Quantum Cryptography: Thomas Pornin, among others, introduced BAT, a post-quantum key encapsulation mechanism, promising better performance than other forthcoming standardized solutions. Additionally, NIST's standardization process for post-quantum cryptographic algorithms, which aims to resist cryptanalysis by quantum computers was discussed by Thomas Pornin.

**The team released multiple post-quantum cryptography papers:**

- Thomas Pornin on Improved Key Pair Generation for Falcon, BAT and Hawk
- Thomas Pornin on BAT: Small and Fast KEM over NTRU Lattices
- Thomas Pornin on Hawk which been submitted to NIST
- Giacomo Pope on A Note on Reimplementing the Castryck-Decru Attack and Lessons Learned for SageMath
- Giacomo Pope on A Direct Key Recovery Attack on SIDH
- Giacomo Pope on FESTA: Fast Encryption from Supersingular Torsion Attacks

Cryptanalysis: Giacomo Pope discussed the implementation of a cryptanalytic attack against SIKE, a finalist of the NIST Post-Quantum Cryptography Project. This attack could break the highest-level security parameters in a short time.

## Crypto Attacks

Cryptography Side Channels: Gérald Doussot explored side channel findings in implementations of the QUIC protocol. The focus was on timing side channels arising from data processing at secret offsets.

Random Number Generators: Paul Bottinelli highlighted the vulnerability in a Pseudo-Random Number Generator (PRNG) based on the ChaCha20 cipher, emphasizing the importance of robust random number generators in cryptographic protocols.

Software Vulnerabilities and Blockchain: Aleks Kircanski examined erroneous computation patterns in Golang, highlighting their implications in blockchain, where they can lead to unintended ledger states or netsplits, which have significant consequences like double-spend attacks.

.

## Signatures & Algorithmic Considerations

Lattice-Based Signatures: In a two-part blog, Elena Bakos Lang provided an intuitive understanding of the two lattice-based signature schemes – Falcon and Dilithium – set for standardization by NIST.

Multivariate Cryptography: Sam Markelon blogged on the topic of multivariate digital signature themes, by walking through an illustrative example of a multivariate digital signature scheme called Unbalanced Oil and Vinegar (UOV) signatures. UOV schemes serve as the basis for a number of contemporary multivariate signature schemes like Rainbow and MAYO.

Cryptography in Practice: Various posts, like the one by Giacomo Pope on the SIAM Conference on Applied Algebraic Geometry, showcased real-world applications and discussions on cryptography. Eli Sohl continued work on Cryptopals video solutions. Paul Bottinelli presented on Selected Cryptography Vulnerabilities of IoT implementations at ICMC 2022. Javed Samuel presented on Practical Cryptography at Geek Week 2023,

Implementation Strategies: Thomas Pornin's blog post shed light on the coding strategy choices during the implementation of cryptographic algorithms on certain elliptic curves, particularly Curve25519.

# Cloud & CI/CD Pipeline Security

Over the course of 2022 and 2023, several NCC Group research outputs on cloud and CI/CD pipeline security emerged from our experts. These studies were a deep dive into the intricacies of ensuring robust cyber defense mechanisms in modern cloud environments, software development and deployment paradigms.

Key themes in this category were:

- Security Vulnerabilities in Modern DevOps: The vulnerabilities in CI/CD pipelines and their real-world implications
- Dynamic Testing and Infrastructure as Code (IaC): The role of dynamic tools in IaC and the complexities they introduce
- Cloud Platform Benchmarks: The efficacy and importance of benchmarks like CIS for cloud platforms such as Microsoft 365, AWS and GCP
- Data Integrity in CRM Platforms: Challenges and best practices for maintaining data integrity in platforms like Salesforce
- Access Control Mechanisms: Evolving authentication and authorization paradigms, particularly in Azure and AWS

> *It's been great to devote more attention to CI/CD and pipeline security research. The era of exploiting Jenkins script console is over and now we can focus on other basics and TOP 10 misconfigurations.-*
> ***Viktor Gazdag, Principal Security Consultant***

Some of our outputs in this domain included:

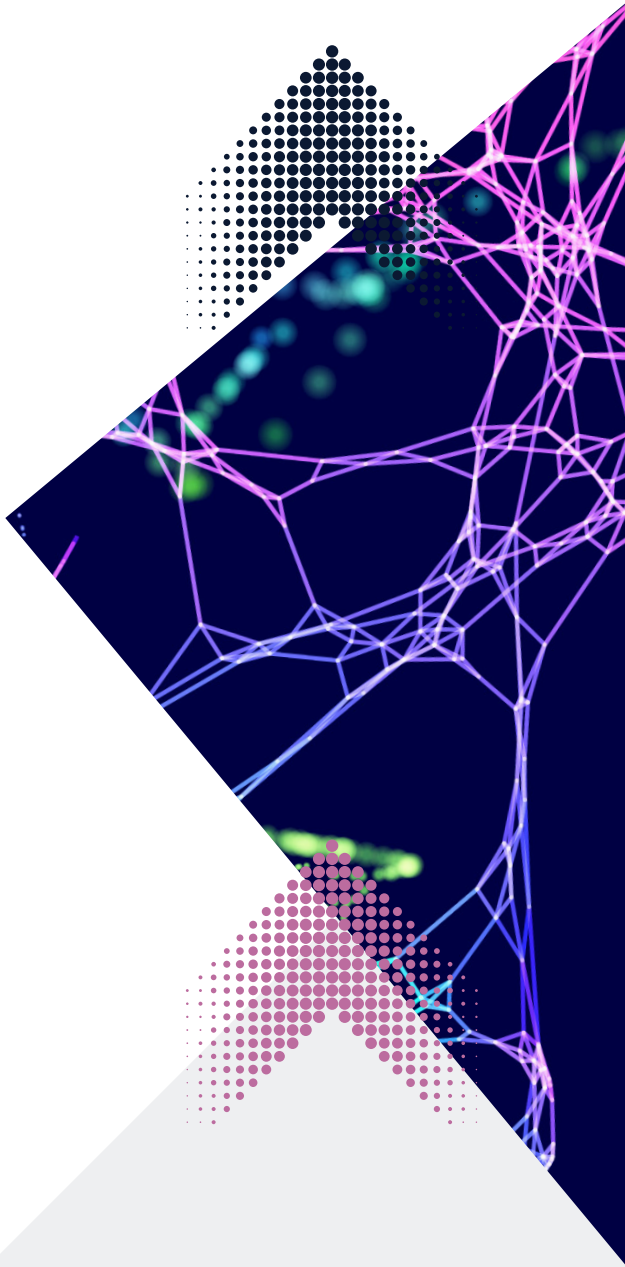
### CI/CD Pipeline Security

Aaron Haymore, Iain Smart, Viktor Gazdag, Divya Natesan and Jennifer Fernick delved into vulnerabilities in CI/CD pipelines by narrating ten real-world scenarios. They found avenues of compromise through means such as vulnerable code, credential theft, or permission abuse. The compromised pipelines could lead to malicious code injections, sensitive data theft, or pipeline disruptions.

### Infrastructure as Code (IaC) Testing

Erik Steringer explored dynamic tooling's role in ensuring the security of IaC. While IaC offers advantages like version control and reusability, it also brings new complexities and potential vulnerabilities. Steringer emphasized integrating robust testing processes with dynamic tools like Inspec, Pulumi, and Terratest.

Viktor Gazdag further contributed to this theme by providing a comprehensive guide on integrating security into infrastructure as a code, emphasizing the significance of security checks, tools, and procedures in cloud automation.



## Cloud Platform Security

Viktor Gazdag evaluated the efficacy of the Center for Internet Security (CIS) benchmarks for Microsoft 365 and the Google Cloud Platform. These benchmarks serve as yardsticks for securing cloud environments against prevalent attack vectors.

Ken Wolstencroft used a threat modeling approach to understand security challenges on Google Cloud Platform (GCP) and point out necessary security controls.

Alberto Verza discussed the evolution of Multi-Factor Authentication in Azure Active Directory, highlighting tools to identify gaps emerging from conditional access policies.

Rennie deGraaf introduced AWS's attribute-based access control, underscoring the innovative use of tags for implementing ABAC.

Luis Toro introduced Post-exploiting a compromised etcd – Full control over the cluster and its nodes, releasing a tool, which includes multiple functions for post-exploitation of compromised etcds.

## Data Integrity and Exception Handling

Jerome Smith explored the challenges related to maintaining data integrity and handling exceptions in the prominent CRM platform Salesforce. He showed how misconfigurations, inadequate exception handling, and flawed data management can lead to data corruption or loss. Jerome also highlighted vulnerabilities in custom Salesforce development, emphasizing the potential for exploitable attack opportunities due to language-specific vulnerabilities.

# Hardware & Embedded Systems

Our hardware and embedded systems security experts engaged in a wide range of research across 2022 and 2023, delving deep into the intricacies of device vulnerabilities, secure development practices, and real-world implications of compromised hardware.

Key themes and observations from this research domain were:

- Early-stage Security: We highlighted the significance of integrating security measures right from the initial stages of hardware and system development
- Vulnerability Analysis: Comprehensive investigation of vulnerabilities in various hardware appliances including printers, routers, and storage devices revealed systemic vulnerabilities
- Secure Boot: Our deep dives into ROM vulnerabilities and secure boot bypasses emphasized the importance of robust initial stages of device operation
- Microcontroller Security: As microcontrollers become ubiquitous in IoT and embedded systems, their security remains paramount

> *Product security cannot be easily added after the product is complete. Engaging your security team early and often is the only cost-effective way to ensure that you are protecting your customers. The system threat model and security requirements need to be understood by the development team before they begin their foundational component selection and implementation decisions. Relying on your chipset and Board Support Package (BSP) vendors to provide a complete security story is rarely viable. -* ***Rob Wood, Global VP for Hardware & Embedded Security***

The overarching message from our research outputs was the imperative, continued need for proactive measures, deep analysis, and consistent vigilance in the domain of hardware and embedded security.

**Firmware Extraction and Analysis**

Catalin Visinescu detailed a methodology to bypass software update package encryption and directly extract the firmware of the Lexmark MC3224i printer. By desoldering the flash from the PCB, it was possible to analyse and retrieve the printer firmware, demonstrating the potential vulnerabilities that exist even when manufacturers take measures to secure their software updates.

**Hardware in the Secure Development Lifecycle**

Rob Wood highlighted the importance of prioritizing security during the early stages of hardware and embedded systems development. By embedding security from inception, developers can evade the pitfalls of potential vulnerabilities. Proactive measures can result in long-term savings, bolstered product reliability, and an enhanced brand reputation. Rob presented the need for thorough threat analysis, security requirements integration, and consistent security testing.

**Microcontroller Security**

In his exploration of the ESP32 microcontroller, Jameson Hyde shed light on potential security challenges and provided a comprehensive guide to implementing secure design principles. These recommendations encompassed secure boot and flash encryption protocols, key management, and secure coding guidelines.

**ROM Vulnerabilities and Secure Boot**

Jon Szymaniak unravelled a ROM-level defect in NXP i.MX application processors that had the potential to exploit the secure boot process. This research underscored additional vulnerabilities that can manifest when ROM-resident authentication code is utilized for a second-stage loader.

Additionally, Ilya Zhuravlev applied some creative fault injection attacks to bypassed secure boot on a UNISOC system-on-chip which is used in millions of Android phones worldwide.

Finally, Sultan Qasim Khan released a technical advisory for the ever-popular U-Boot bootloader, describing how a physical attacker can compromise a device during the USB-based firmware update process.

**BIOS Analysis**

Jeremy Boone embarked on an in-depth analysis of Intel's Alder Lake BIOS, exposing a time-of-check-time-of-use (TOCTOU) vulnerability in a SMI handler, which posed a high risk of privilege escalation. Another Intel BIOS vulnerability was discovered which was unique due to it being remotely exploitable over Bluetooth. Finally, Jeremy delved into the vulnerabilities present in Insyde Software's System Management Mode (SMM) modules, discovering vulnerabilities that impact hundreds of laptop models across multiple vendors.

### Memory Security Concerns

Rob Wood discussed the paramount importance of addressing security concerns with regards to modern memory technologies, when designing embedded systems. Neglecting these concerns can lead to significant data compromises.

### Platform Root of Trust

Jeremy Boone embarked on an audit of AMI's Tektagon Open Edition, an open-source Platform Root of Trust (PRoT) solution. This research emphasized the role of hardware root-of-trust (HRoT) in maintaining firmware integrity.

### Bluetooth

Sultan Qasim Khan developed a new type of Bluetooth Low Energy (BLE) relay attack operating at the link layer, enabling low latency relaying of BLE connections with and without link layer encryption release in a trifecta of technical advisories. The capabilities of this relay made it possible to defeat proximity authentication on several targets resistant to prior relay attack tooling. This relay attack was publicly demonstrated against several targets, including the Tesla Model 3 and Y, and Kwikset/Wiser Kevo smart locks, for which technical advisories describing their susceptibility and possible mitigations approaches were published. NCC Group disclosed details to companies behind the affected products researched before publicly releasing technical details – we have been discussing mitigation approaches with the Bluetooth Special Interest Group (SIG).

# Operating System Security

Quite a few of our research projects across 2022 and 2023 related to Operating System security. Key themes and insights from these research projects were:

- Enhancing Security Through Modern Languages: The adoption of Rust as a safer alternative to traditional languages continues, specifically regarding kernel and driver development
- Forensic Capabilities: We developed tools and methodologies to aid forensic investigations, particularly related to Microsoft Windows telemetry
- Detection Mechanisms: We performed research aimed at detecting subversive techniques used by malicious software, such as implant frameworks
- Memory and Boot Chain Integrity: Ensuring the security of memory processes, from handling exceptions to boot chains in operating systems and devices can sometimes still be challenging for modern operating systems
- Bypassing Existing Security Measures: We performed detailed insights into how some security mechanisms, like DEP, can potentially be bypassed, aiming to identify and rectify such vulnerabilities

> *Our team's rigorous exploration into Windows and Linux telemetry and memory integrity, and the transformative potential of languages like Rust, reflects our unwavering commitment to advancing the field of future OS security, which is not just about defending but about proactively understanding, anticipating, and innovating.* - ***Matt Lewis, Global Head of Research***

Anomalous Vectored Exception Handlers Detection on Windows: we researched post-exploitation frameworks using Vectored Exception Handling (VEH) on Microsoft Windows to subvert hook detection. One such discovery led to Ollie Whitehouse's creation of a "Copy on Write Detector" capable of identifying patches in the traditional memory patching process. This allows us to enumerate and identify potentially malicious VEH handlers. The shared code can verify if a process uses VEH, which handlers are present, which modules they point to, and whether they point to known modules.

Windows Telemetry and Customer Interaction Tracker (CIT): Up until Windows version 7, a telemetry source named Customer Interaction Tracker was present. The CIT database, when parsed, can aid in forensic investigations. Erik Schamper provided code to parse the CIT database and integrated these findings into an investigation framework to handle various evidence data.

Detection Opportunities for Windows Implant Framework: Ollie Whitehouse's research shared insights through a lightning talk on opportunities to detect implant framework behaviours on Windows.

FreeBSD Kernel Module in Rust: Modern languages like Rust provide enhanced security by eliminating common memory safety security bugs. David Young's research looked at community efforts towards this and presented a basic proof-of-concept kernel module for FreeBSD developed in Rust.

Rustproofing Linux: With Rust's introduction to the Linux Kernel, there's anticipation that developers will port or create new device drivers in Rust. Domen Puncer Kugler's four-part research series investigated the security dynamics of porting a Linux device driver from C to Rust. Through this, five vulnerable drivers in C were transitioned to Rust to explore potential vulnerability persistency after the porting.

Bypassing Windows DEP with a Custom ROP Chain: Alex Zaviyalov delved into the crafting of a custom ROP chain to circumvent Windows 10's Data Execution Prevention (DEP).

# Exploit Development Group

NCC Group's Exploit Development Group (EDG) is a small team of full-time exploit developers who write custom exploits exclusively for the purpose of helping our clients test their own infrastructure and systems using real-world attacks against contemporary vulnerabilities to better understand their risk and resilience.

EDG often present their research externally and occasionally will speak publicly about advanced vulnerability research and exploitation. In recent years, they have been enjoying great success in the prestigious Zero Day Initiative Pwn2Own competitions, finishing third place in the 2022 Pwn2Own Toronto competition.

Key EDG research outputs in 2022 and 2023 included:

- Router, Printers and NAS Vulnerabilities: A major focus was on exploring vulnerabilities in consumer routers (such as TP-Link, Netgear, Synology), small business routers (Ubiquiti) and in enterprise printers (Lexmark and Canon) and network attached storage (Western Digital)
- Exploit Development and Methodology: Multiple EDG presentations were given at global tier-1 conferences and concentrated on exploit development techniques, methodologies, and the tools employed
- Linux Kernel Security: The team identified several Linux kernel security vulnerabilities and outlined ways to exploit them
- Training & Secondments: Internal NCC Group secondments were provided to NCC Group employees to develop their exploitation skills, while free, advanced exploitation training was incorporated into the Open Security Training 2 Platform

> *EDG is conscious of advanced attackers targeting networking devices in the wild over recent years. This together with more industry awareness of the exploitation of 0-day security issues has changed the security landscape and methods needed for defence. EDG's research into these areas and fundamental core technologies (i.e., the Linux kernel) which underpin critical infrastructure allows NCC Group to stay up to date with advanced exploitation techniques and provide pragmatic guidance to NCC Group's customers.* - ***Alex Plaskett (Security Researcher)***

Over the last few years, many employees have ended up working within remote environments. With this comes additional security challenges - what was once the enterprise network perimeter is expanded to consumer devices with questionable security. EDG's research has highlighted significant weaknesses in a number of these consumer devices and demonstrates how a sufficiently advanced attacker is able to remotely compromise, laterally move to internal networks and maintain persistence using vulnerabilities unknown to the vendor. Overall, EDG research outputs represented cutting-edge explorations in the world of advanced vulnerability exploitation and development:

At NCC Group's internal conference "NCC Con Europe 2022" in Spain, Cedric Halbronn, Aaron Adams, Alex Plaskett and Catalin Visinescu delivered two presentations, allowing the wider NCC Group research community to grasp the methodology and approach adopted for vulnerability research, especially with regards to the Pwn2Own competition. The talk covered approaches from both hardware and software security and demonstrated why it is important to consider both aspects in embedded systems security.

Alex Plaskett and Cedric Halbronn unveiled research dubbed "Toner Deaf – Printing your next persistence" at Hexacon 2022. Their talk revolved around the remote network-based exploitation of a Lexmark printer, demonstrating how an attacker could maintain access to a compromised printer across firmware updates and restarts. The team also published a detailed blog in this area.

McCaulay Hudson found and disclosed multiple vulnerabilities in consumer routers. The first, "MeshyJSON: A TP-Link tdpServer JSON Stack Overflow", and the second, "Puckungfu: A NETGEAR WAN Command Injection". Both vulnerabilities were discovered during the preparation phase for the Pwn2Own competition.

McCaulay delved further into the NETGEAR vulnerability in his article on the NETGEAR RAX30 router: "NETGEAR Routers: A Playground for Hackers?" Which provided a detailed look at the security vulnerabilities inherent in NETGEAR's custom binaries. While McCaulay pointed out various security lapses, he also acknowledged the security measures implemented by NETGEAR, making several vulnerabilities challenging to exploit. EDG also published another detailed blog post on another Netgear remote vulnerability which Netgear released patches to address.

Another critical presentation, "HITBAMS – Your Not so 'Home' Office – Soho Hacking at Pwn2Own", by Alex Plaskett and McCaulay Hudson spotlighted the endeavours of EDG in Pwn2Own targeting consumer routers and using this to pivot to compromise devices on the internal network. This involved exploiting both LAN and WAN perspectives and then using this compromise to move laterally and attack other devices on the network.

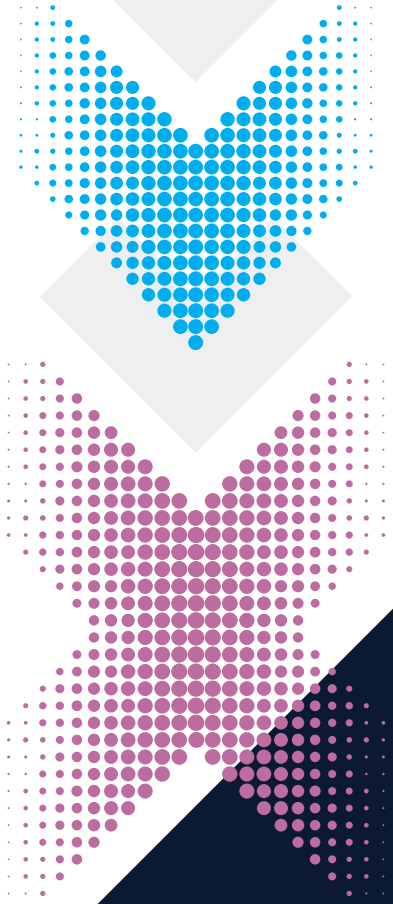
The Linux kernel was the focal point for EDG at OffensiveCon 2023. Cedric Halbronn and Alex Plaskett illuminated the audience on "Exploit Engineering – Attacking the Linux Kernel". Over the last year EDG found and exploited 3 privilege escalation vulnerabilities against a fully patched OS with all mitigations enabled. The most recent vulnerability was patched against versions of the kernel going back 6 years, demonstrating that exploitable issues can exist in highly critical operating system software for long periods of time. The team also published an in-depth blog in this area.

EDG also published an in-depth article on exploiting Western Digital NAS (which they had performed the previous year at Pwn2Own) using a memory corruption issue in an open-source library (Netatalk) which was used on the NAS. This issue together with other vulnerabilities lead to the vendor removing the Netatalk service to reduce attack surface on the device.

Alex Plaskett later presented at @SysPWN on "SysPWN – VR for Pwn2Own", giving insights into the Pwn2Own competition from various perspectives. The talk was segmented into two sections, the first section discussing high level experience and learning in Pwn2Own and the latter part delving into the vulnerabilities that NCC Group EDG leveraged during the 2021 and 2022 Pwn2Own events.

On the training side Cedric Halbronn successfully launched his class on Windows Kernel Exploitation on the Open Security Training 2 Platform. The class teaches how to exploit a race condition vulnerability leading to a use-after-free in the Kernel Transaction Manager (KTM) component of the Windows kernel. It shows the approach an exploit developer should take in attacking a previously unresearched component in the Windows kernel.

Aaron Adams presented at HITB Phuket 2023, detailing the exploitation of two PostScript vulnerabilities in Lexmark printers as successfully used during Pwn2Own 2022 Toronto. The talk delved into the internals of an interpreters (PostScript) functionality and highlighted how an advanced attacker could use this to gain access to Lexmark devices.



# Collaboration with Industry & Academia

In the rapidly evolving landscape of cyber threats, fostering a collaborative approach to cybersecurity research has become more crucial than ever. By leveraging the collective expertise and diverse perspectives of industry peers and academic institutions, NCC Group has significantly enriched its knowledge base, stimulated innovative solutions, and accelerated the development of advanced cybersecurity tools and methodologies. These research collaborations not only bolster our ability to safeguard against emerging threats but also serve as a testament to the power of unity in addressing the complex challenges posed by the digital age.

Some examples of this collaboration from the past couple of years include:

**Quantum Datacenter of the Future**

NCC Group is a key participant in the UK Research & Innovation (UKRI) 3-year funded Quantum Data Centre of the Future project, a comprehensive consortium led by ORCA Computing and consisting of 14 organizations and universities. This initiative aims to seamlessly incorporate quantum communication and computing systems into classical data centers, revolutionizing the future of data storage and processing. KETS Quantum Security continues to develop quantum key distribution and random number generation capabilities for the datacenter, a project on which NCC Group has been providing crucial security architecture and design support.

**Working with UCL on AI/ML Cyber Research**

Since 2017, NCC Group has been working with University College London's (UCL) Centre for Data Intensive Science and Industry (DISI), situated within their Department of Physics and Astronomy. DISI serves as a vital conduit for nurturing and engaging MSc and PhD students in AI research, training, and the facilitation of knowledge transfer between the academic and industrial sectors. In 2022, we provided a six-month full-time placement for a final year PhD student within DISI, providing them with a range of cutting-edge research challenges in the realm of AI and Machine Learning. During this placement, PhD student Nikolay Walters developed a tool using Natural Language Processing (NLP) techniques and the pre-trained CodeBERT model to identify exposed secrets and crypto miners in source code. Additionally, Nikolay created an email ecosystem powered by OpenAI's GPT-3, capable of generating and replying to emails automatically.

**IoT & Equity, Inclusion & Sustainability with Edinburgh University**

Leveraging insights from Human-Computer Interaction, Design, and Law, in 2022 we committed research support to an Engineering and Physical Sciences Research Council (EPSRC) consortium research grant to discern future challenges and conceive equitable IoT solutions. Led by the University of Edinburgh, other collaborators include UK consumer champion Which?, BBC Research & Development, and the Department of Employment and Social Development in the Canadian Government.

This interdisciplinary project, spanning two years, is delving into the growing concerns surrounding the lack of repairability in the consumer Internet of Things (IoT) and its potential repercussions on equity, inclusion, and sustainability in the digital landscape. As IoT devices become increasingly prevalent, there is an emergent risk of a digital divide, especially for lower-income households, stemming from the non-durability of these devices, poor cybersecurity, data misuse, and environmental unsustainability. Output from the research will derive a toolkit that offers comprehensive guidelines for manufacturers, policymakers, and the general community to champion more sustainable and equitable IoT practices.

> *NCC Group is committed to engaging with governments as they make important decisions about future cyber policy that affects us and our clients. Our Research enables us to talk to politicians and senior decision-makers from a position of authority, presenting arguments for better cyber rules and regulations that are well-evidenced and based in the realities that our Research reveals. Ultimately, our Research is fundamental to our ability to be a trusted advisor to governments around the world.*
> ***Verona Hulse, UK Head of Government Affairs***

**LoRaWAN Research with the University of Surrey**

In collaboration with the University of Surrey, NCC Group was involved in developing tools for the trackability of LoRaWAN networks. The Fine-Grained Trackability in Protocol Executions paper outlines how FLoRa (a LoRaWAN Testing Framework developed by NCC Group) extension was implemented by the University of Surrey to create new trackability/privacy attacks on these, with proposed countermeasures.

### Ruling the Rules – Understanding Network Intrusion Detection Systems (NIDS)

Mathew Vermeer, a doctoral candidate at the Organization Governance department of the faculty of Technology, Policy and Management of Delft University of Technology provided a summary of a study conducted as part of his PhD research, performed in collaboration with Fox-IT. The research studied the different processes and technologies that determine or impact the security posture of organizations. The research set out to understand efficacy of the signature-based network intrusion detection system (NIDS).

### UK Department for Science, Innovation & Technology (DSIT) and Enterprise IoT Security

In response to the rising prevalence of 'smart' devices in office environments, in October 2022, the UK's Department for Science, Innovation & Technology (DSIT) initiated a research project with NCC Group to assess the cybersecurity risks posed by popular enterprise connected devices utilized by UK businesses. These devices, if compromised, could potentially grant attackers access to sensitive business data. The investigation involved testing these devices against current security principles and guidelines to gauge their resilience against evolving cyber threats. Findings from our research revealed various alarming vulnerabilities, including prevalent outdated software, with one instance being over 15 years old. A total of 1 critical and 9 high-risk vulnerabilities were identified across 8 tested devices, some of which could allow full access to a device's camera or the ability to monitor and record VoIP calls. Moreover, our study found that a higher price does not necessarily equate to better security, highlighting the need for further policy and legislative considerations in this domain.

> *"Working in collaboration with our academic partners, industry colleagues and customers enables NCC Group to deliver leading edge cybersecurity research greater than the sum of its parts. By bringing the experience and expertise of our consultants we can provide unique industry perspective on some of the biggest challenges facing cybersecurity now and into the future. This can be clearly seen in our recent outputs working on applications of quantum computing, AI and the Internet of Things with fantastic recognition of the value of our work in enterprise IoT in the recent UK Cabinet Office National Cyber Strategy Annual Progress Report."* ***Jon Renshaw, Deputy Director of Commercial Research***

# Other Interesting Research

NCC Group consultants engaged in other interesting discreet research projects throughout 2022 and 2023. From decoding the intricacies of vulnerability management in diverse coding languages to confronting the pressing cybersecurity demands in the healthcare sector, our findings underscore the critical role of reverse engineering in security research, the complexities of modern networking, and the indispensable role of secure programming in today's digital landscape.

Highlight outcomes from these projects include:

- Vulnerability Detection & Management: Many of our research projects focused on understanding, detecting, and managing vulnerabilities, whether they're in coding languages, applications, or systems
- Healthcare Cybersecurity: We had a specialized focus on the unique cybersecurity challenges posed by the healthcare industry, particularly in the realm of connected medical devices
- Reverse Engineering: Several of our research outputs pivoted around the importance and methods of reverse engineering to understand and potentially exploit software systems
- Modern Networking & Security: We explored security concerns in emerging and prevalent networking solutions like 5G and DNS systems
- Secure Programming & Development: Many of our research outputs involved the promotion of safe programming languages and methodologies to avert common security and safety pitfalls in software development

Further detail on some of these interesting research projects includes:

Vulnerabilities in Coding Languages: Nick Dunn collated existing knowledge on double fetch vulnerabilities in C and C++, detailing their various forms, their occurrences, and potential fixes.

Cybersecurity in Healthcare: Stuart Kurutac's literary review "Understanding the Impact of Ransomware on Patient Outcomes" delved into the impact of cyberattacks on patient outcomes in healthcare, pointing to a significant research gap in the long-term effects of such attacks. In the blog post "Medical Devices: A Hardware Security Perspective", Jameson Hyde highlighted the unique challenges of securing an expanding array of connected medical devices, discussing the regulatory landscape's attempts to ensure their safety.

Detection and Defense Mechanisms: In "Detecting Mimikatz with Busylight", Balazs Bucsay unveiled a novel method of detecting Mimikatz, a well-known credential-harvesting application, by emulating a specific USB device.

State of DNS Rebinding in 2023: Roger Meyer presented an updated analysis on DNS rebinding attacks, examining the effects of various internet technologies and introducing a new draft specification aiming to prevent such attacks.

Reverse Engineering and Game Security: In "Reverse Engineering Coin Hunt World's Binary Protocol", Quentin Chambers provided a detailed walkthrough on reverse engineering parts of the Android game, Coin Hunt World, with the aim to develop tools that can cheat at the game.

5G Network Security: Philip Marsden explained the primary security threats to 5G networks, highlighting the vulnerabilities discovered during penetration testing and consultancy engagements.

Decompilation and P-Code Analysis: In "Exploring Ghidra's decompiler internals", James Chambers inspected the Ghidra decompiler's internals, discussing the nuances of P-Code simplification styles and how to debug its application.

Bug and Exploit Analysis: In "Replicating CVEs with KLEE", Mark Tedman demonstrated how to replicate and exploit a previously reported bug, underscoring the importance of timely software patching to prevent potential attacks.

The Demystifying Cobalt Strike's "make_token" Command post explains the inner workings of Cobalt Strike's "make_token" command, as well as its use cases and limitations. Not a lot of public information exists about this functionality, which has some "gotchas" and, sometimes can result in undesirable outcomes for an operator.

# Acknowledgements

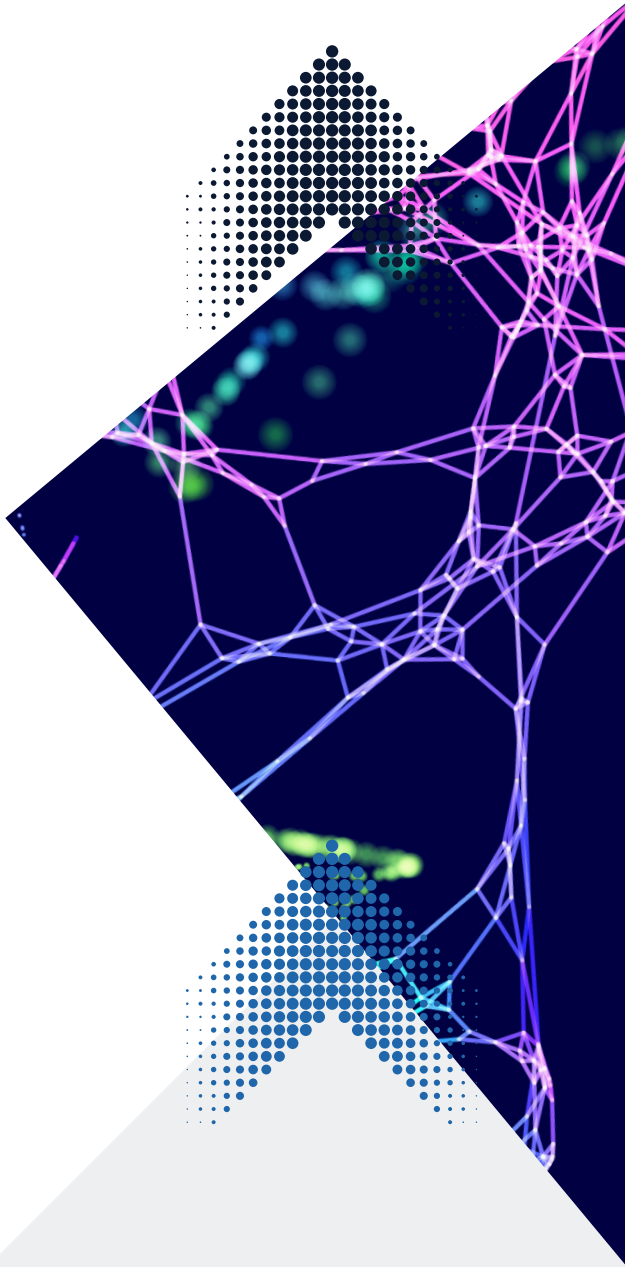
Research is an intrinsic part of many of our technical security consultants' daily lives, and almost all of the research in this report was delivered by dozens of consultants at NCC Group locations around the world, seconded into research to work on their passion projects, empowered by thousands of dedicated research days across the Group.

Our first acknowledgement goes out to all our consultants who spent part of their time in the research division over the past few years, without whose talent, curiosity, time, and courage our research simply would not exist. Thanks also to the many researchers and consultants who provided input and review of this report.

Immeasurable thanks to Ristin Rivera, our Research Program Coordinator, for their invaluable contributions to our research program, including help with countless coordinated vulnerability disclosures, administrative and program management support.

Huge gratitude to our global research leads Daniel Romero, Chris Anley, Jeremy Boone, Sultan Qasim Khan and William Groesbeck for their support of NCC Group's research program and mentoring of NCC Group researchers.Sincere thanks to Jon Renshaw for his great work driving NCC Group's client-funded research.

Lastly, we would like to thank Jennifer Fernick, who led NCC Group's Research Program as Global Head of Research until November 2022. Under her guidance, the NCC Group Research Program published well over 600 research talks, blogs, papers, tools and advisories. Her vision set the Research Program to grow and most of the research presented in this report and conducted during 2022 was performed under her purview.



# About Research at NCC Group

NCC Group employs some of the most talented security consultants and researchers on the planet, serving 15,000 clients worldwide and uncovering countless vulnerabilities per year through both client work and independent vulnerability research.

With hundreds of specialized consultants, our technical security research areas extend into almost every area of security, as well as global standards bodies including CIS Benchmarks. We perform offensive and defensive research across a vast range of targets including blackbox and whitebox testing of previously unanalyzed emerging technologies and computational architectures. We publish research in a variety of subfields including applied cryptography, hardware and embedded systems, secure coding and programming languages, browser and client-side security, cyber-physical systems, operating systems and their internals, mobile security and privacy, application security, privacy enhancing technologies, distributed systems, network and protocol security, cloud, containerization, and virtualization, and both offensive attacks on – and defensive uses of – machine learning and AI systems.

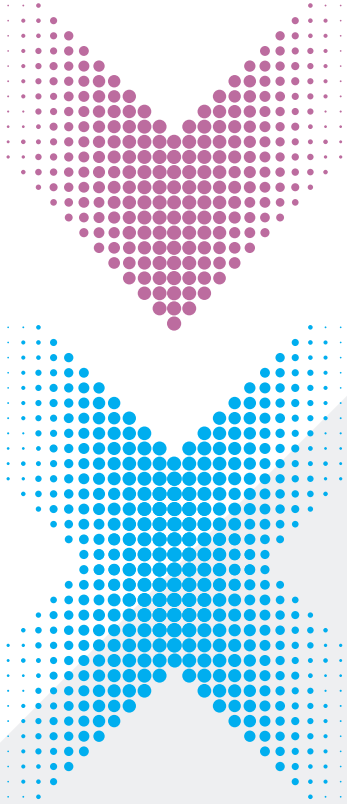
You can find samples of some of our recent public-facing work, including blog posts, whitepapers, conference talk listings, and technical advisories on our Research Blog, alongside our technical Twitter (X) account and our public GitHub which hosts over 300 open-source tools and datasets authored by NCC Group researchers. We also have deep academic research partnerships with several leading universities, as evidenced across several of our research publications. NCC Group also regularly conducts publicly reported security audits across a range of high impact and security-critical technologies.

Our technical capabilities extend beyond our public-facing work, to include our internal-only groups and resources, including our world-class Exploit Development Group (EDG), Threat Intelligence Team and Full Spectrum Attack Simulation (FSAS) group, as well as several technical specialty practices and hundreds of pieces of unpublished proprietary tooling.

Our research program delivers thousands of research days annually, by researchers at all levels from across our global business. We support our researchers through a full-time technical research leadership team, mentorship and coaching, incentives and awards, and collaboration within and across several internal research groups. We regularly present our work in top research venues including Black Hat USA, Shmoocon, Hardwear.io, REcon, Appsec USA, Toorcon, BSidesLV, Chaos Communication Congress, Microsoft BlueHat, HITB Amsterdam, RSA Conference, CanSecWest, OffensiveCon, DEF CON, and countless others. Our research is regularly covered by publications including Wired, Forbes, The New York Times, Politico, DarkReading, Techcrunch, Fast Company, the Wall Street Journal, The Register, SC Magazine, and other mainstream and trade publications globally.

research.nccgroup.com

@nccgroupinfosec



# Appendices

## Appendix 1: Open-Source Security Tool & Code Releases

Between 2022 and 2023 we released over 21 open-source security tools, major tool updates, implementations, or other open-source repositories. Our tools provide insight or efficiency gains across several distinct areas of cybersecurity. Among the open-source tools released by NCC Group during this period were:

**Cloud & Container Security**

- Insject: A tool for poking at containers. It enables users to run an arbitrary command in a container or any mix of Linux namespaces

- Aerides: An implementation of infrastructure-as-code (IaC) scanning using dynamic tooling. This tool demonstrates how to integrate LocalStack and dynamic tools for assessing IaC. It includes mock infrastructure for a web service written using Terraform's HCL

- Monkey 365: A security tool to conduct Microsoft 365 and Azure subscriptions and Azure Active Directory security configuration reviews without the significant overhead of learning tool APIs or complex admin panels from the outset

- Project Kubescout: Adding Kubernetes Support to Scout Suite - ScoutSuite scanning capability for Kubernetes clusters

- ScoutSuite 5.12.0: Scout Suite can now also scan Kubernetes clusters. Scout Suite is an open source multi-cloud security-auditing tool, which enables security posture assessment of cloud environments. Using the APIs exposed by cloud providers, ScoutSuite gathers configuration data for manual inspection and highlights risk areas

- ScoutSuite 5.13.0: This version includes multiple new rules and findings for Azure, which align with some of the latest CIS Benchmark checks, multiple bug fixes and feature enhancements, and minor finding template corrections. Supported Python versions have also been updated to cover versions 3.9 and newer

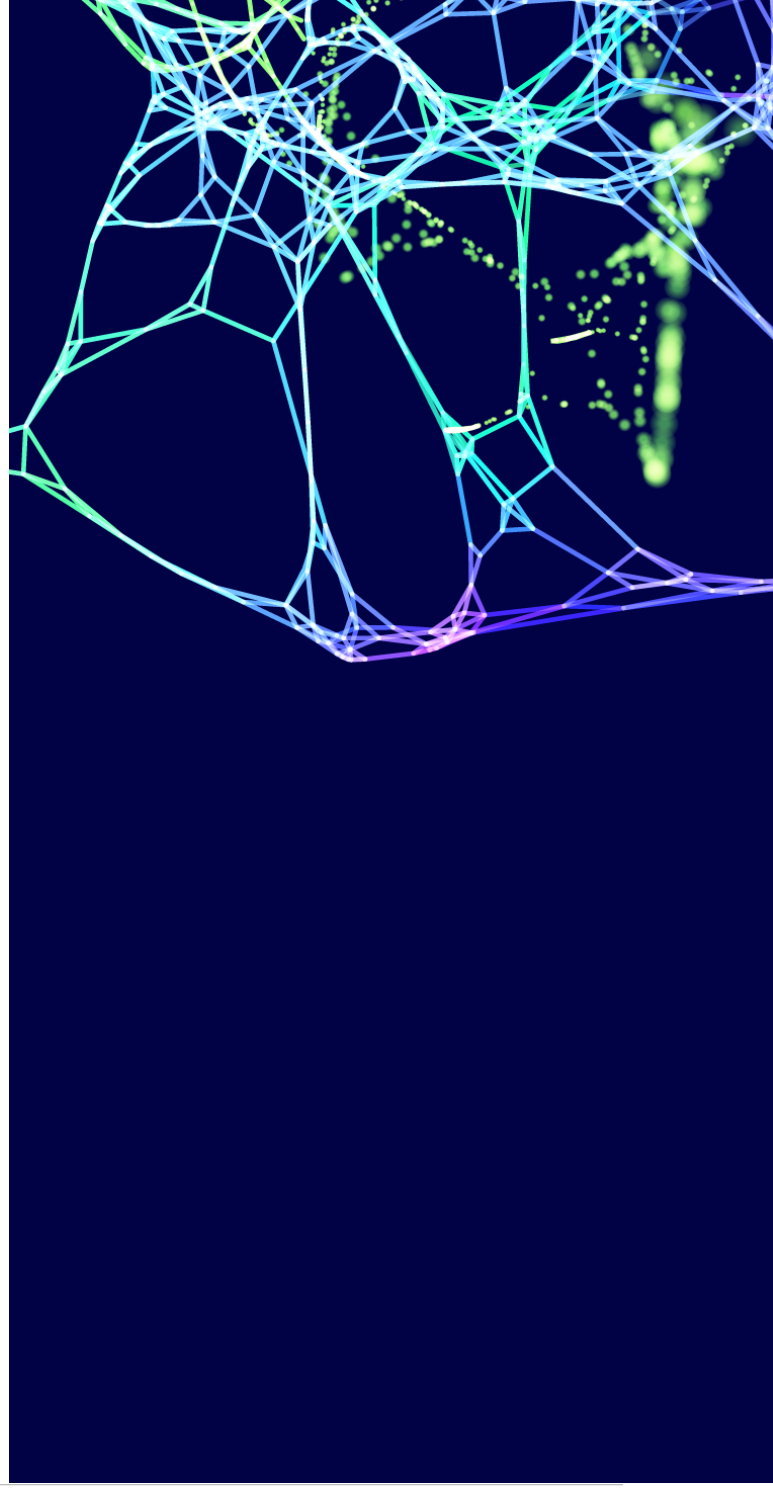
- CowCloud: A serverless solution to distribute workloads in AWS. CowCloud was created to run recon tools and vulnerability scans in a distributed way; for example, one use case might be by bug bounty hunters. This solution abstracts end users from the underlying work required to distribute workloads in AWS. CowCloud provides users with a friendly web interface to view and create new tasks consumed by Python code running on worker nodes (EC2 instances)

- Kubetcd: It automates pod deployment by writing directly into etcd. It includes multiple functions for post-exploitation of compromised etcds.

**Binary & Code Analysis**

- Ghostrings: A set of scripts for recovering string definitions in Go binaries with P-Code analysis. Tested with x86, x86-64, ARM, and ARM64

- Castryck-Decru Key Recovery Attack on SIDH: A reimplementation of this attack it in SageMath; a free, open-source mathematics software system



• Code Credential Scanner (ccs): This script is intended to scan a large, diverse codebase for hard-coded credentials, or credentials present in configuration files. These represent a serious security issue, and can be extremely hard to detect and manage

• Code Query (cq): A universal code security scanning tool. CQ scans code for security vulnerabilities and other items of interest to security-focused code reviewers. It outputs text files containing references to issues found, into an output directory. These output files can then be reviewed, filtered by unix command line tools such as grep, or used as a means to 'jump' into the codebase at the specified file:line reference

• Cartographer: A code coverage mapping plugin for Ghidra, enabling researchers to observe which parts of a program have been executed without requiring source code

• LibSLUB: A python library to examine the SLUB management structures and object allocations (the Linux kernel heap implementation) python library to examine the SLUB management structures and object allocations (the Linux kernel heap implementation)

• Exploit Mitigations: EDG continued to maintain a list of exploitation mitigations over time in various operating systems, software, libraries and hardware

**Web & Network Interactions**

• JWT ReAuth Version 1.0.0: Provides Burp with a way to authenticate with a given endpoint, parse out the provided token and then attach it as a header on requests going to a given scope

• Web3 Decoder: A Burp Suite Extension that helps to analyze what is going on with the operations involving smart contracts of the web3. This is mainly JSON-RPC calls to Ethereum Nodes, and nodes of other compatible networks (like Polygon, Arbitrum, BSC...)

• DroppedConnection: Emulates a Cisco ASA AnyConnect VPN service, accepting any credentials (and logging them) before serving VBS to the client that is executed in the context of the user

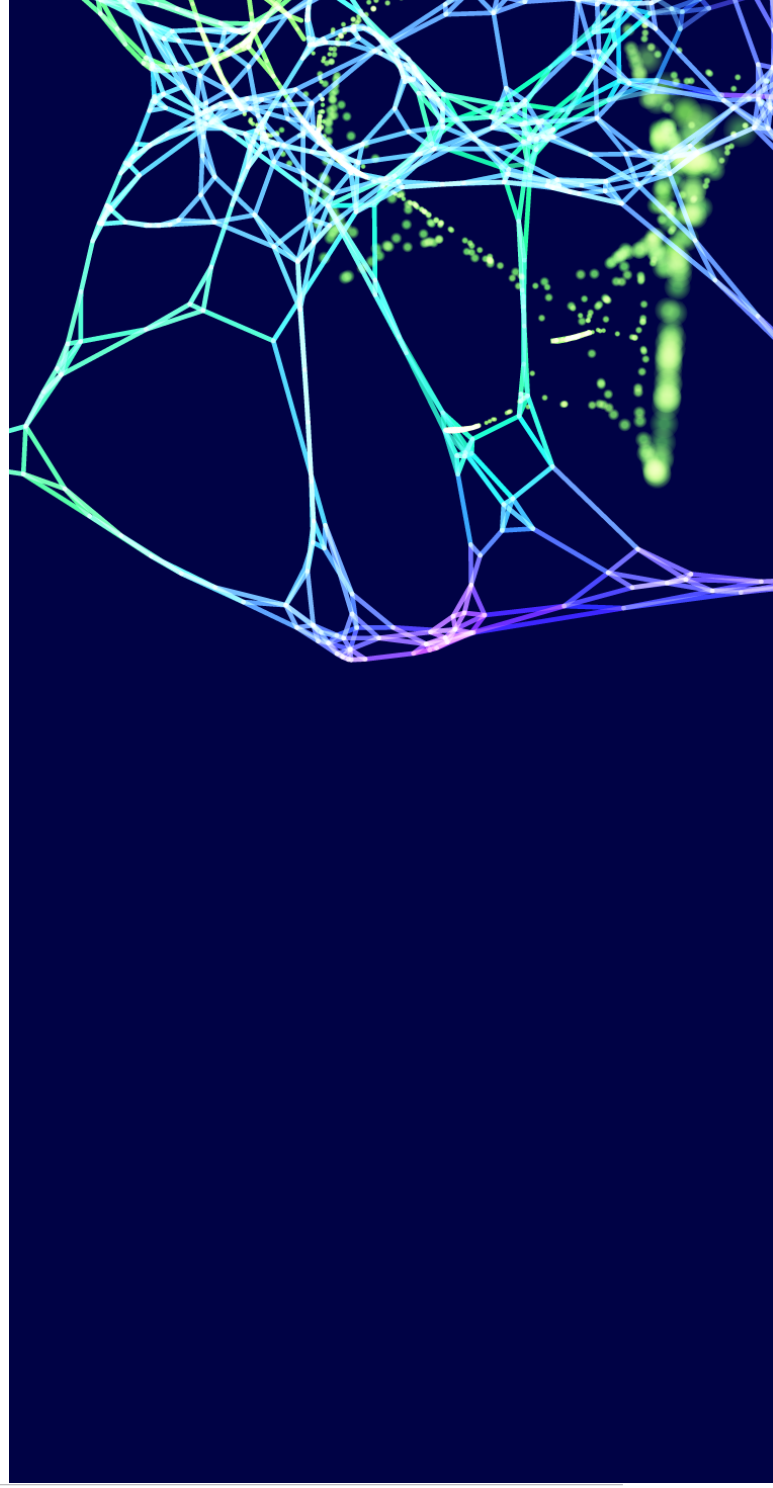
• Magisk module - Conscrypt Trust User Certs: This module makes all installed user certificates part of the APEX module com.android.conscrypt certificate store in Android 14, so that they will automatically be used when building the trust chain.

**Data Extraction & Monitoring**

• Mimikatz Detector: ConDrv is a device created by condrv.sys, which handles the traffic between the Console Application (cmd/powershell/etc) and the actual console (conhost.exe). Console Monitor is a C# GUI application that shows the end user every keystroke or line sent to or from the console

• Mimikatz detector driver: A USB HID driver emulation with PID/VID (0x3bca/0x27bb) of Plenom A/S Busylight Alpha supported by Mimikatz

• MetadataPlus: A tool to extract metadata from Microsoft Office files that includes new locations not checked in other tools



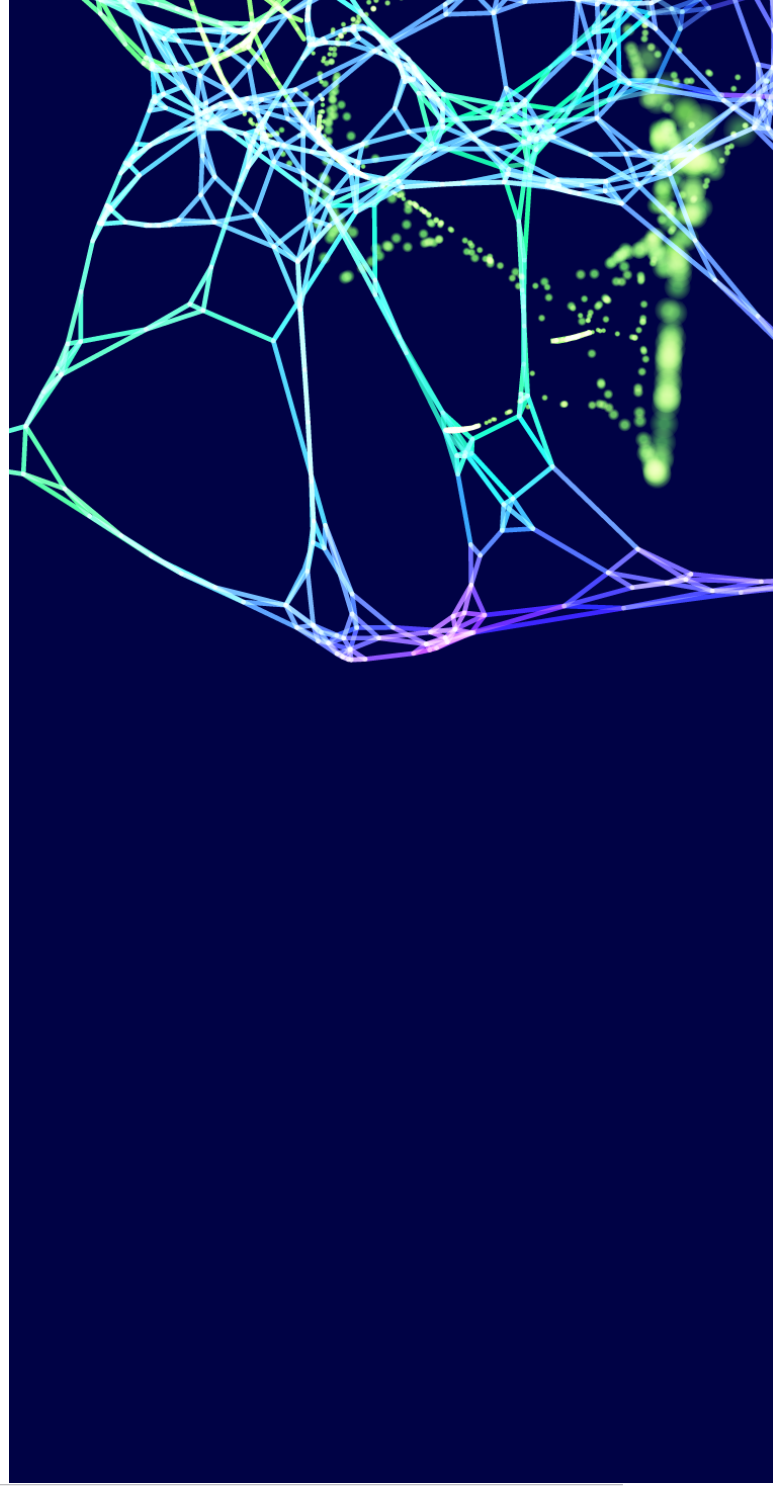
## Appendix 2: Publicly Reported Security Audits

Each year NCC Group releases several security audits of vital open-source software components and certain proprietary systems, resulting from paid engagements with our clients. By making these reports public, organizations can offer transparency to their end-users regarding the security of key products and system components. This openness not only assures regulators, auditors, and legislators of product and system security strengths but also demonstrates the organization's commitment to proactive security measures, especially by seeking evaluations from independent third-party security experts like NCC Group.

Between 2022 and 2023, NCC Group delivered over 18 Public Reports across several different cryptographic implementations, as well as for key security functions and controls in products and systems of Google, AWS, Kubernetes and many others.

Our 2022 - 2023 Public Reports included:

- O(1) Labs Mina Client SDK, Signature Library and Base Components Cryptography and Implementation Review
- Google Enterprise API Security Assessment
- go-cose Security Assessment
- Lantern and Replica Security Assessment
- Threshold ECDSA Cryptography Review
- Penumbra Labs Decaf377 Implementation and Poseidon Parameter Selection Review
- IOV Labs powHSM Security Assessment
- Google Confidential Space Security Review
- VPN by Google One Security Assessment
- Solana Program Library ZK-Token Security Assessment
- Kubernetes 1.24 Security Audit
- AWS Nitro System API & Security Claims
- Zcash Zebra Security Assessment
- Penumbra Labs R1CS Implementation Review
- Entropy/Rust Cryptography Review
- Caliptra Firmware Security Assessment
- Zcash FROST Security Assessment
- WhatsApp Auditable Key Directory (akd) Implementation Review



## Appendix 3: Technical Advisories

In an era where our dependence on technology has never been more pronounced, the vigilance in detecting vulnerabilities within the digital systems and tools we use daily has become paramount. This section sheds light on over 69 security vulnerabilities uncovered in various products, a testament to the rigorous research endeavors our team undertook throughout 2022 and 2023. Vulnerability research is not merely an academic exercise; it plays a pivotal role in ensuring the digital safety of individuals, businesses, and nations. Each vulnerability identified presents an opportunity for malicious entities to exploit and compromise systems, leading to data breaches, financial losses, and even threats to human safety.

The Common Vulnerabilities and Exposures (CVE) process stands as a keystone in the security landscape. By assigning a unique identifier to each vulnerability, the CVE system provides a standardized way of sharing and communicating the nature and severity of threats. Equally crucial is the act of responsible vulnerability disclosure. This ensures that vendors are made aware of potential flaws in their systems and are given an opportunity to address them, thus strengthening the overall security posture of their products. The patches and fixes that arise from this collaborative process between researchers and vendors are emblematic of the collective effort required to fortify our digital world against evolving threats.

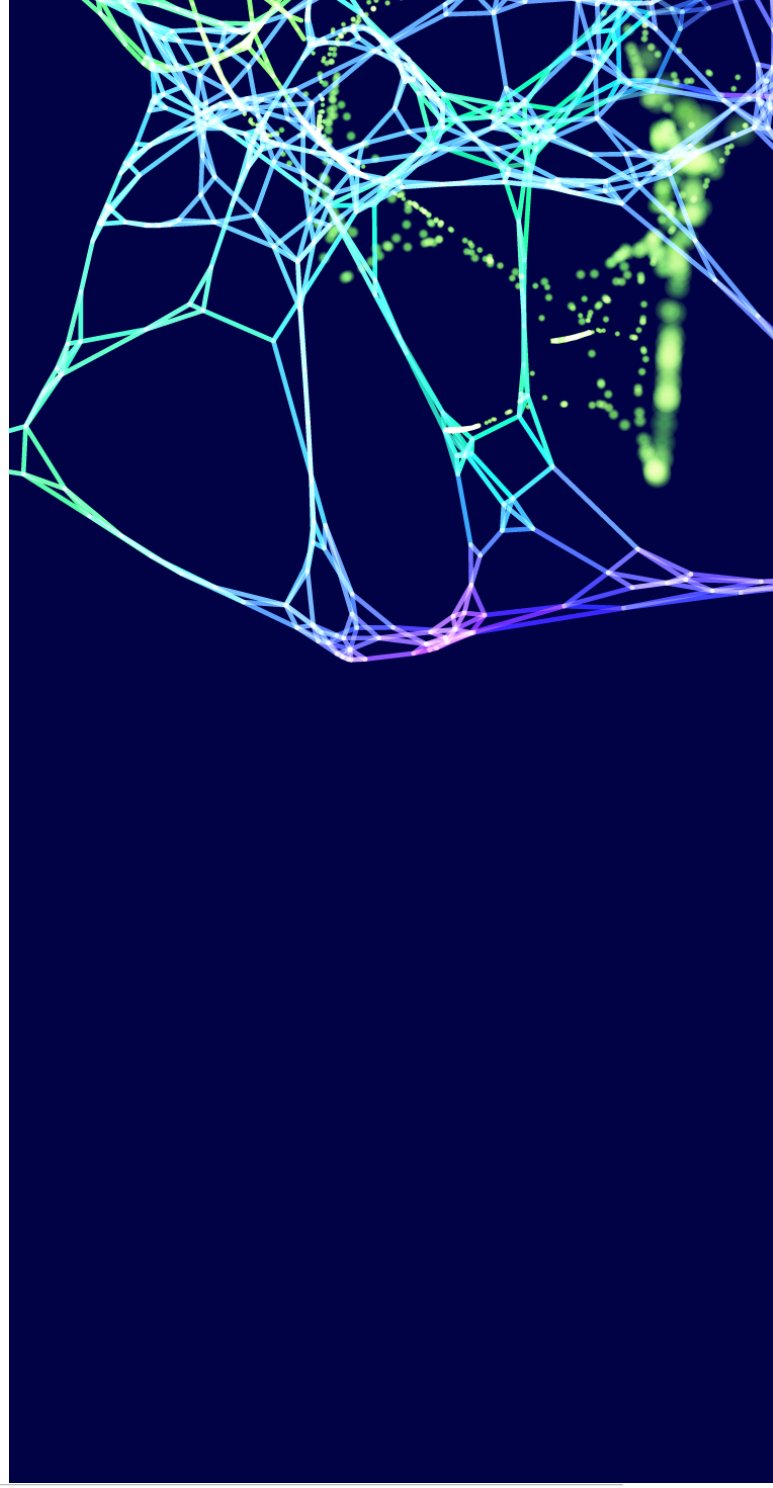
Key themes that emerged across the vulnerabilities found include:

- Remote Exploits: Many of the vulnerabilities related to Remote Code Execution and Authenticated Remote Command Execution, which focus on the ability of an attacker to remotely execute arbitrary code on a target system

- Memory Issues: Several of the vulnerabilities related to how software manages memory, highlighting gaps in secure development lifecycles and/or programmer security training. These vulnerabilities can lead to data leaks, crashes, or even the execution of arbitrary code

- Input Validation: A recurring theme was improper handling of input. Failing to validate or sanitize inputs can allow attackers to inject malicious code, access unauthorized data, or disrupt system operations

- Multiple Vulnerabilities: Several products were affected by “Multiple Vulnerabilities,” meaning that they were exploitable via several different classes of vulnerability. That modern products can be so vulnerable and exposed, often out-of-the-box is alarming and attests to disregard for principles of security by the product manufacturers



The following table highlights vulnerabilities identified in third party products during 2022 and 2023:

| Platform | Vulnerability | CVE(s) / Vendor Response | NCC Group Researcher(s) |
|---|---|---|---|
| Apple macOS XAR | Arbitrary File Write | CVE-2022-22582 | Richard Warren |
| Ruby on Rails | Possible XSS Vulnerability in ActionView tag helpers | CVE-2022-27777 | Álvaro Martín Fraguas |
| Bluetooth Low Energy (BLE) | Proximity Authentication Vulnerable to Relay Attacks | April 2022: Response from Bluetooth SIG confirming that relay attacks are a known risk, and that more accurate ranging mechanisms are under development | Sultan Qasim Khan |
| Tesla | BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks | April 2022: Response from Tesla Product Security stating that relay attacks are a known limitation of the passive entry system | Sultan Qasim Khan |
| Kwikset/Weiser | BLE Proximity Authentication in Kevo Smart Locks Vulnerable to Relay Attacks | **October 2021: Discussion with broader Spectrum Brands HHI engineering team regarding attack setup details and mitigation approaches** | Sultan Qasim Khan |
| SerComm h500s | Multiple Vulnerabilities | CVE-2022-30325<br>CVE-2022-30326<br>CVE-2022-30327<br>CVE-2022-30328<br>CVE-2022-30329 | Andrea Shirley-Bellande |
| FUJITSU CentricStor Control Center <= V8.1 | Vulnerabilities allow for hijack of control link | March 2022: Pull request rejected by ExpressLRS maintainer; differing opinions between NCC Group and developers | Richard Appleby |
| U-Boot | Multiple Vulnerabilities | CVE-2022-30790<br>CVE-2022-30552 | Nicolas Bidron, and Nicolas Guigo |
| Trendnet TEW-831DR WiFi Router | Multiple Vulnerabilities | CVE-2022-30325<br>CVE-2022-30326<br>CVE-2022-30327<br>CVE-2022-30328<br>CVE-2022-30329 | Andrea Shirley-Bellande |

| Platform | Vulnerability | CVE(s) / Vendor Response | NCC Group Researcher(s) |
|---|---|---|---|
| ExpressLRS | Vulnerabilities allow for hijack of control link | March 2022: Pull request rejected by ExpressLRS maintainer; differing opinions between NCC Group and developers | Richard Appleby |
| Nuki smart locks | Multiple Vulnerabilities | CVE-2022-32509<br>CVE-2022-32504<br>CVE-2022-32502<br>CVE-2022-32507<br>CVE-2022-32503<br>CVE-2022-32510<br>CVE-2022-32506<br>CVE-2022-32508<br>CVE-2022-32505 | Daniel Romero, Pablo Lorenzo and Guillermo del Valle |
| Unisoc ROM | Several Unpatchable Vulnerabilities | CVE-2022-38693<br>CVE-2022-38694<br>CVE-2022-38695<br>CVE-2022-38696<br>CVE-2022-38691<br>CVE-2022-38692 | Ilya Zhuravlev |
| Juplink RX4-1800 WiFi Router | Multiple Vulnerabilities | CVE-2022-37413<br>CVE-2022-37414 | Jennifer Reed |
| OpenJDK | Weak Parsing Logic in java.net. InetAddress and Related Classes | **June 2022: The Oracle Security Alerts team stated that their "evaluation is that this is an input validation issue and we are scoring it as a CVSS 0"** | Jeff Dileo |
| NXP i.MX | SDP_READ_DISABLE Fuse Bypass | CVE-2022-45163 | Jon Szymaniak |
| Galaxy App Store | Improper Access Control and Improper Input Validation | CVE-2023-21433<br>CVE-2023-21434 | Ken Gannon |
| U-Boot | Unchecked Download Size and Direction in USB DFU | CVE-2022-2347 | Sultan Qasim Khan |

| Platform | Vulnerability | CVE(s) / Vendor Response | NCC Group Researcher(s) |
|---|---|---|---|
| Insyde System Management Mode | Memory Corruption, No Check before Use, Attacker Controlled Write, Insufficient Input Validation | CVE-2023-22616<br>CVE-2023-22612<br>CVE-2023-22615<br>CVE-2023-22613<br>CVE-2023-22614 | Jeremy Boone |
| Faronics Insight | Multiple Vulnerabilities | CVE-2023-28344<br>CVE-2023-28345<br>CVE-2023-28346<br>CVE-2023-28347<br>CVE-2023-28348<br>CVE-2023-28349<br>CVE-2023-28350<br>CVE-2023-28351<br>CVE-2023-28352<br>CVE-2023-28353 | Oliver Brooks |
| Nullsoft Scriptable Installer System (NSIS) | Insecure Temporary Directory Usage | July 2023: NSIS version 3.09 released | Richard Warren |
| Intel BIOS | Memory Corruption in HID Drivers | CVE-2022-44611 | Jeremy Boone |
| Tektagon OpenEdition | Out-of-bounds read and write<br>Lack of Input Validation | As of April 6th 2023, these vulnerabilities were fixed in commit d6d935e. No CVEs were issued by AMI. | Jeremy Boone |
| SonicWall Global Management System (GMS) & Analytics | Multiple Critical Vulnerabilities | CVE-2022-45163 | Jon Szymaniak |

| Platform | Vulnerability | CVE(s) / Vendor Response | NCC Group Researcher(s) |
|---|---|---|---|
| SonicWall Global Management System (GMS) & Analytics | Multiple Critical Vulnerabilities | March 2022: Pull request rejected by ExpressLRS maintainer; differing opinions between NCC Group and developers | Richard Appleby |
| Juplink RX4-1800 WiFi Router | Multiple Vulnerabilities | CVE-2023-34133<br>CVE-2023-34124<br>CVE-2023-34123<br>CVE-2023-34137<br>CVE-2023-34127<br>CVE-2023-34134<br>CVE-2023-34125<br>CVE-2023-34126<br>CVE-2023-34129<br>CVE-2023-34135<br>CVE-2023-34132<br>CVE-2023-34128<br>CVE-2023-34136<br>CVE-2023-34131<br>CVE-2023-34130 | Richard Warren, Sean Morland |
| Connectize G6 AC2100 Dual Band Gigabit WiFi Router | Multiple Vulnerabilities | CVE-2023-24046<br>CVE-2023-24047<br>CVE-2023-24048<br>CVE-2023-24049<br>CVE-2023-24050<br>CVE-2023-24051<br>CVE-2023-24052 | Jay Houppermans |
| Proxyman | Network redirection | CVE-2023-45732 | Scott Leitch |
| Western Digital PR4100 NAS | Unchecked Return Value – Remote Code Execution | CVE-2022-23121 | EDG |
| Trendnet TEW-831DR WiFi Router | Multiple Vulnerabilities | CVE-2022-30325<br>CVE-2022-30326<br>CVE-2022-30327<br>CVE-2022-30328<br>CVE-2022-30329 | Andrea Shirley-Bellande |

| Platform | Vulnerability | CVE(s) / Vendor Response | NCC Group Researcher(s) |
|---|---|---|---|
| Ubiquiti Networks | EdgeOS dhcp6c Command Injection Remote Code Execution Vulnerability | CVE-2023-23912 | EDG |
| Lexmark MC3224i | Remote and Arbitrary Code Execution Persistence after reboot | CVE-2023-26063<br>CVE-2023-26066<br>CVE-2022-29850 | EDG |
| Linux Kernel | A use-after-free vulnerability was found in the Linux kernel's Netfilter subsystem. This flaw allows a local attacker with user access to cause a privilege escalation issue | CVE-2022-32250 | EDG |
| Netgear WAN | WAN Remote Code Execution | No CVE due to Pwn2Own competition entry. Netgear firmware version 1.0.9.90 remediates the issue | EDG |
| Adobe ColdFusion WDDX | Deserialization | CVE-2023-44353 | McCaulay Hudson |
| Sonos Era 100 | U-Boot allowed for persistent arbitrary code execution | No CVE | Alex Plaskett |

## Appendix 4: Conferences & Talks

Each year, our researchers have the distinguished opportunity to present at a series of premier cyber security conferences across the globe, covering a vast array of technologies and exposing critical security vulnerabilities. These symposiums serve as fertile grounds for knowledge sharing and transfer, wherein we engage with the brightest minds in cybersecurity to disseminate our findings and absorb novel insights from peers. Speaking at these conferences not only bolsters our reputation as thought leaders but also catalyzes the challenging of established notions and fosters robust collaborations. It is in these dynamic environments that we not only impart our expertise but also subject it to the invaluable scrutiny of the global community, refining our approaches and sparking innovative research ideas. The dialogue established here extends beyond the confines of the event, cultivating a network of professionals dedicated to the advancement and fortification of our digital world. Through these interactive platforms, we have both contributed to and drawn from the collective intelligence, ensuring that we remain at the vanguard of cybersecurity research and development.

Across 2022 and 2023 our researchers presented at over 32 global conferences, many of which were Tier-1 cyber security research conferences.

| Title | Venue | Researcher(s) |
|---|---|---|
| Popping Locks, Stealing Cars, and Breaking a Billion Other Things: Bluetooth LE Link Layer Relay Attacks | EdHardwear.io | Sultan Qasim Khan |
| Toner deaf - Printing your next persistence | Hexacon | Cedric Halbronn, Alex Plaskett |
| CatchM3ifuKan - Detecting Command-and-Control Techniques Up and Down the Networking Stack with Streaming Statistical and Machine Learning Techniques | Zeek Week | Bispham, Ruud, Joost |
| Alternative ways to detect mimikatz | RootCon | Balazs Bucsay |
| War stories of Jenkins Security Assessments | DevOps World 2022 | Viktor Gazdag |
| Selected Cryptography Vulnerabilities of IoT Implementations (E32a) | ICMC | Paul Bottinelli |
| Shooting Yourself In The Boot - Common Secure Boot Mistakes | BSides St. John's | Jeremy Boone |
| Alternative ways to detect mimikatz | ResponderCon | Balazs Bucsay |
| Enterprise IR: Live free, live large | Sans CyberThreat | Ollie Whitehouse, Eric Schamper |
| Settlers of Netlink: Exploiting a limited kernel UAF on Ubuntu 22.04 to achieve LPE | HITB | Aaron Adams |
| Settlers of Netlink: Exploiting a limited kernel UAF on Ubuntu 22.04 to achieve LPE | Hitcon | Aaron Adams |
| Pursuing Phone Privacy Protection | DEF CON Crypto & Privacy Village | Matt Nash, Mauricio Tavares (non-NCC Group) |
| Hidden Payload in Cyber Security | Black Hat Arsenal 2022 | Chantel Sims |
| Responding to Microsoft 365 security reviews faster with Monkey365 | Black Hat Arsenal 2022 | Juan Garrido |
| MacAttack - A client/server framework with macro payloads for domain recon and initial access | Black Hat Arsenal 2022 | Chris Nevin |
| RCE-as-a-Service: Lessons Learned from 5 Years of Real-World CI/CD Pipeline Compromise | Black Hat Arsenal 2022 | Iain Smart, Viktor Gazdag |
| Cybersecurity, intrusion detection and Machine Learning (LINK) | Summer School Valencia 2022 | Jose Selvi |
| Mastering Container Security | 44CON | NCC Group |
| Google Cloud Platform (GCP) Security Review | 44CON | NCC Group |
| Preparing for Zero-Day: Vulnerability Disclosure in Open Source Software (Panel with OpenSSF Vulnerability Disclosure WG) | Linux Security Summit North America | Jennifer Fernick (NCC Group), Christopher Robinson (Intel), Anne Bertucio (Google) |

| Title | Venue | Researcher(s) |
|---|---|---|
| Securing Open Source Software - End-to-End, at Massive Scale, Together | Open Source Summit North America | Jennifer Fernick (NCC Group), Christopher Robinson (Intel) |
| War stories of Jenkins Security Assessments | DevOps World 2022 | Viktor Gazdag |
| Using machine learning to map CVEs to MITRE ATT&CK | Linux Foundation Global Security Vulnerability Summit | Mostafa Hassan |
| Secure Coding in C | Nullcon Berlin | Robert Seacord |
| Reversing the Pokémon Snap Station without a Snap Station | Shmoocon (postponed from January) | James Chambers |
| You Got This: Stories of Career Pivots and How You Can Successfully Start Your Cyber Career | WiCys 2022 | Alma Rinasz |
| Preparing for Zero-Day: Vulnerability Disclosure in Open Source Software (Panel with OpenSSF Vulnerability Disclosure WG) | FOSS Backstage | Jennifer Fernick (NCC Group), Christopher Robinson (Intel), Anne Bertucio (Google) |
| Microsoft 365 APIs Edge Cases for Fun and Profit | RootedCon | Juan Garrido |
| I'm in your pipes, stealing your secrets | Securi-Tay | Iain Smart |
| Mapping and Attacking Active Directory | Securi-Tay | Derek Price |
| Understanding a Payload's Life | EuskalHack | Daniel López |
| Abusing ETCD: Injecting resources into (almost) unrestricted k8s | EuskalHack | Luis Toro |

# About us

## People powered, tech-enabled, Cyber Security

NCC Group is a global cyber business, operating across multiple sectors and geographies.

We're a research-led organisation, recognised for our technical depth and breadth; combining insight, innovation, and intelligence to create maximum value for our customers.

As society's dependence on connectivity and the associated technologies increases, we help organisations to assess, develop and manage their cyber resilience posture to confidently take advantage of the opportunities that sustain their business growth.

**Contact Us:**
+44 (0) 161 209 5200
www.nccgroup.com
Matt.Lewis@nccgroup.com

XYZ Building
2 Hardman Boulevard
Spinningfields
Manchester

nccgroup