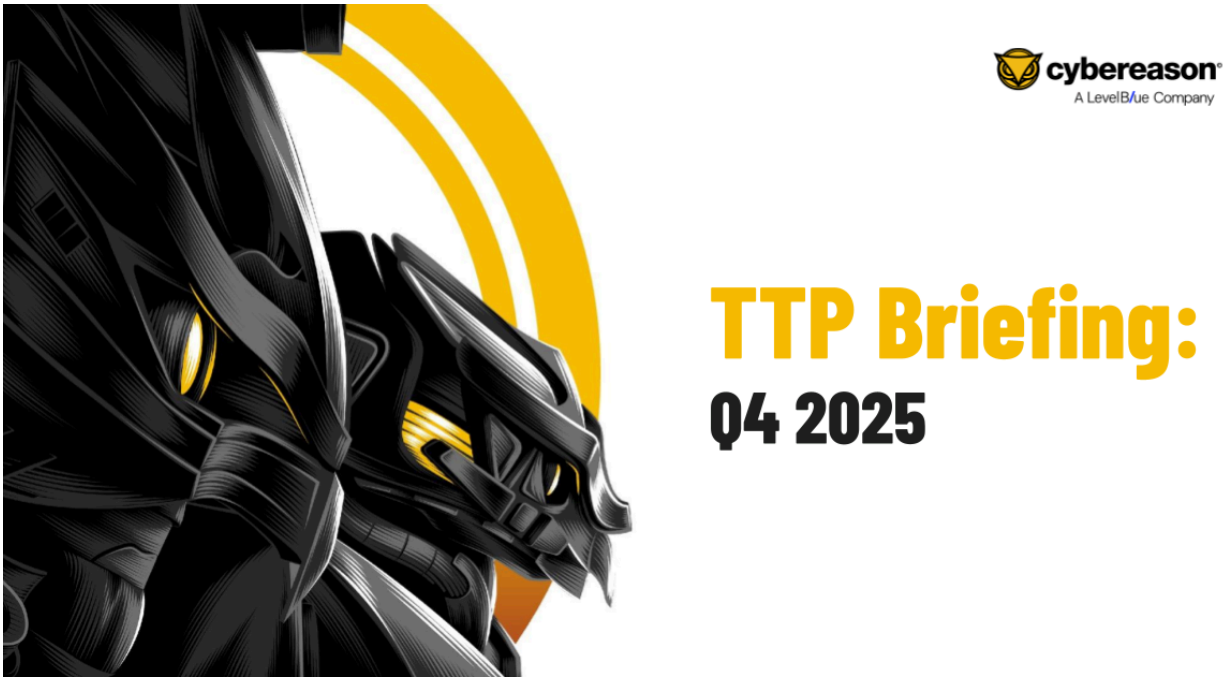
Cybereason Blog | Cybersecurity News and Analysis

By Cybereason

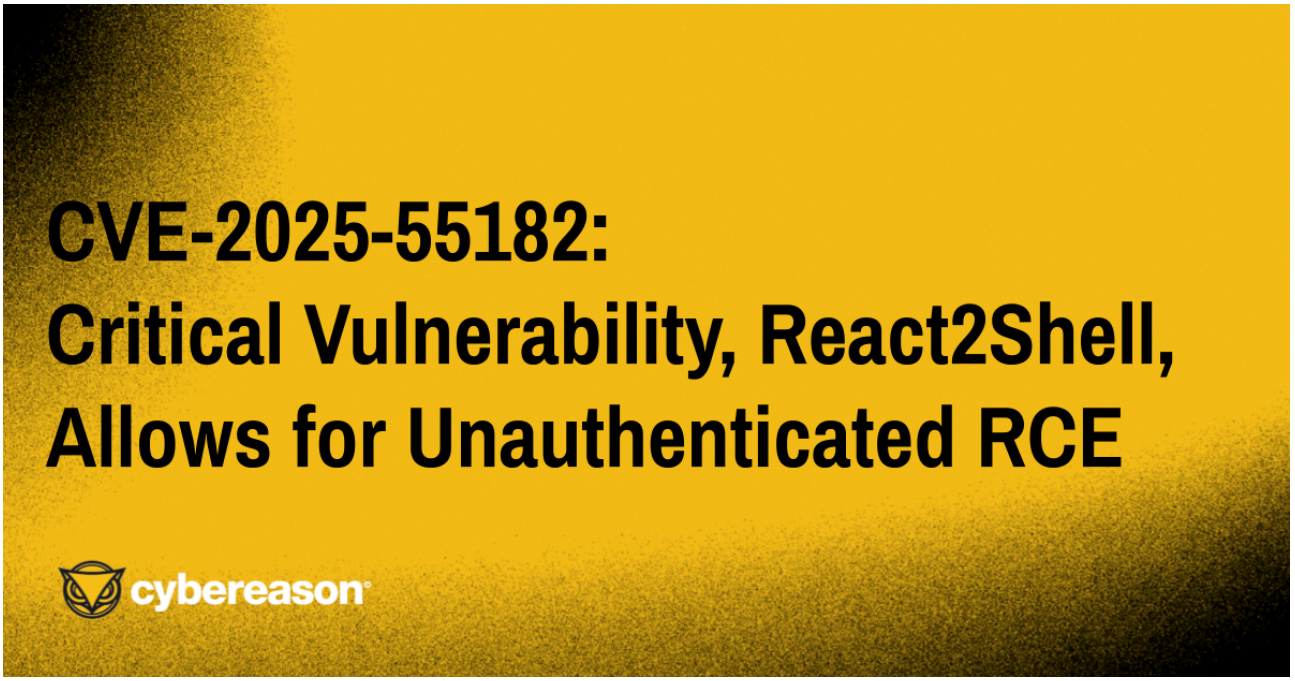
Archived: 2026-04-05 14:51:22 UTC

- Home




IDENTITY & BEYOND:
2026 Incident Response Predictions
cybereason
A LevelBlue Company


MITRE | ATT&CK Evaluations
ENTERPRISE
2025
cybereason
A LevelBlue Company
100% Detection
100% Visibility
100% Accuracy
100% SOC Efficiency

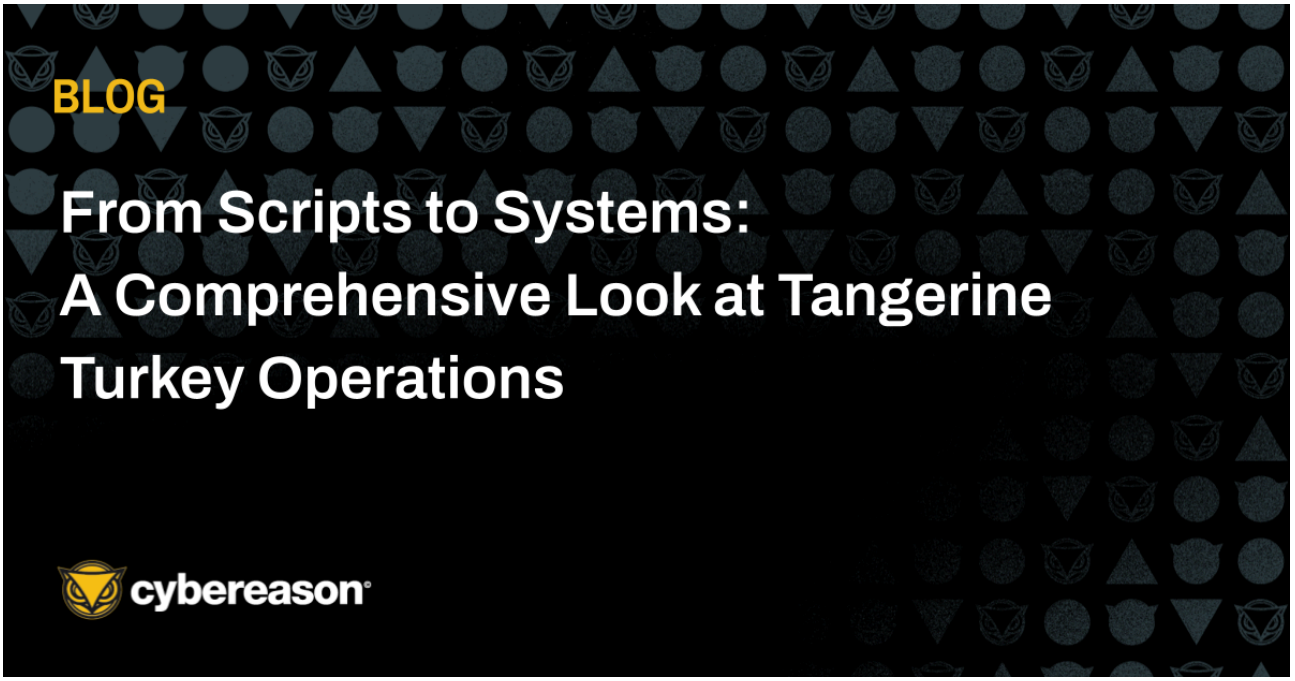

CVE-2025-55182:
Critical Vulnerability, React2Shell,
Allows for Unauthenticated RCE
cybereason


BLOG
License to Encrypt:
“The Gentlemen” Make Their Move
cybereason

[Tycoon 2FA Phishing Kit Analysis]

In this Threat Alert, Cybereason analyzes Tycoon 2FA phishing kit, a sophisticated phishing-as-a-service platform designed to bypass two-factor authentication.

November 3, 2025 / 7 minute read



cybereason

TTP Briefing:
Q3 2025


cybereason
7000+ IRs LATER:
The 11 Essential Cybersecurity Controls


BLOG
Behind the Mask of Madgicx Plus:
A Chrome Extension Campaign
Targeting Meta Advertisers
cybereason

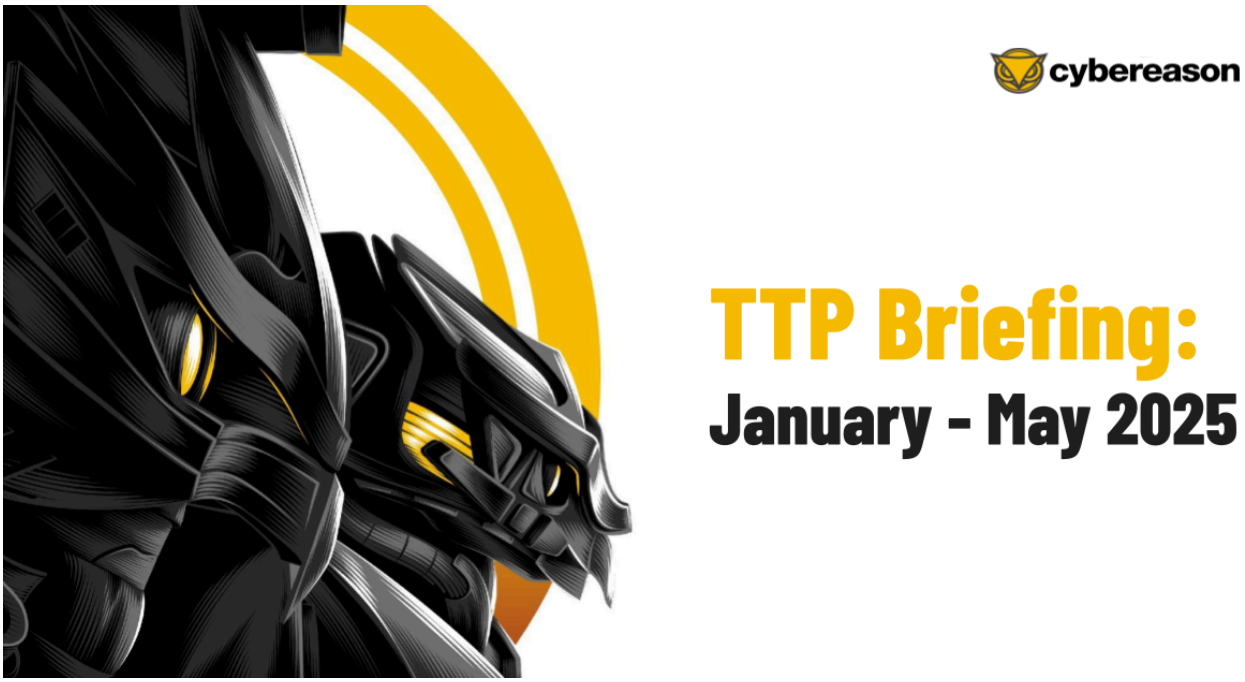

TTP ALERT
CVE-2025-53770 & CVE-2025-53771: Critical On-Prem SharePoint Vulnerabilities
cybereason


BLOG
BlackSuit: A Hybrid Approach with Data Exfiltration and Encryption
cybereason

[Deploying NetSupport RAT via WordPress & ClickFix]

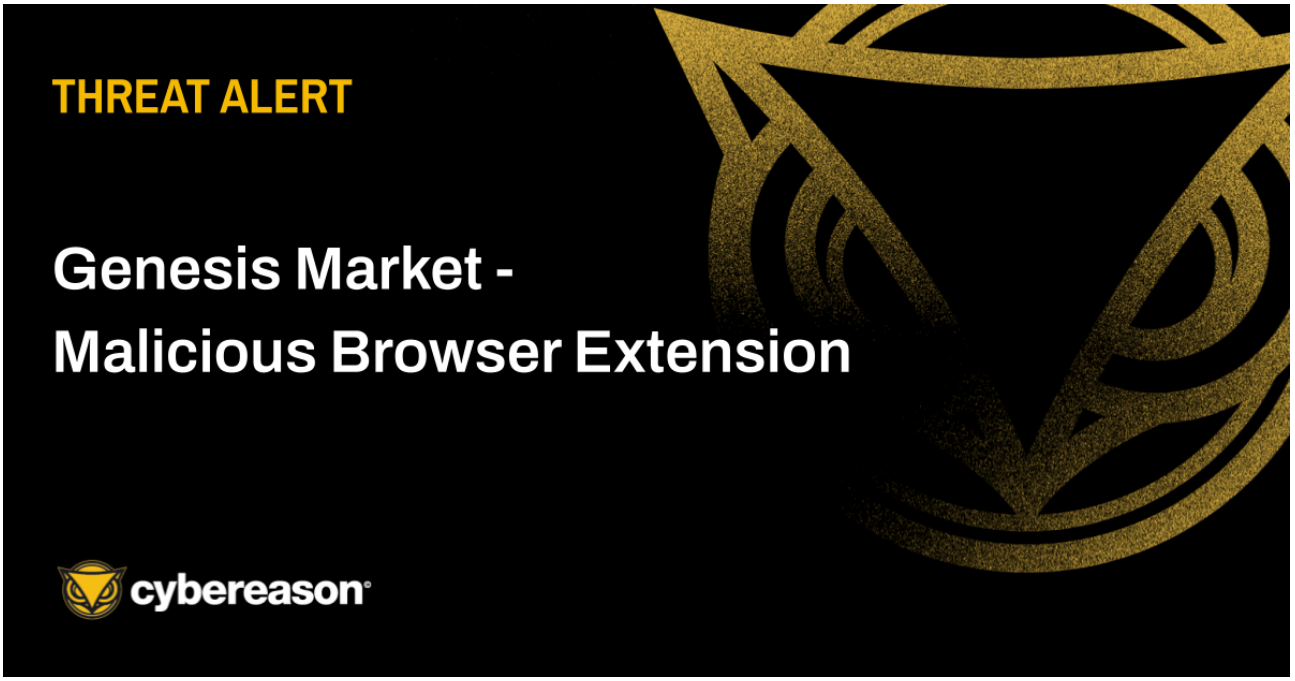
In this Threat Alert, Cybereason analyzes malicious WordPress websites and the methods and tools used by threat actors to deploy the NetSupport Remote Access Tool (RAT) payload.

July 7, 2025 / 5 minute read




THREAT ALERT
Ransomware Gangs Collapse as Qilin Seizes Control
cybereason
QILIN


THREAT ALERT
Copyright Phishing Lures Leading to Rhadamanthys Stealer Now Targeting Europe
cybereason


THREAT ALERT
Genesis Market -
Malicious Browser Extension
cybereason


TTP ALERT
CVE-2025-32433:
Vulnerability Discovered in
Erlang/OTP's SSH Implementation
cybereason


BLOG
From Shadow to Spotlight:
The Evolution of LummaStealer and
Its Hidden Secrets
cybereason


BLOG
A Class Above: Expert Support for Data
Breach Class Action Defense
cybereason

[The Curious Case of PlayBoy Locker]

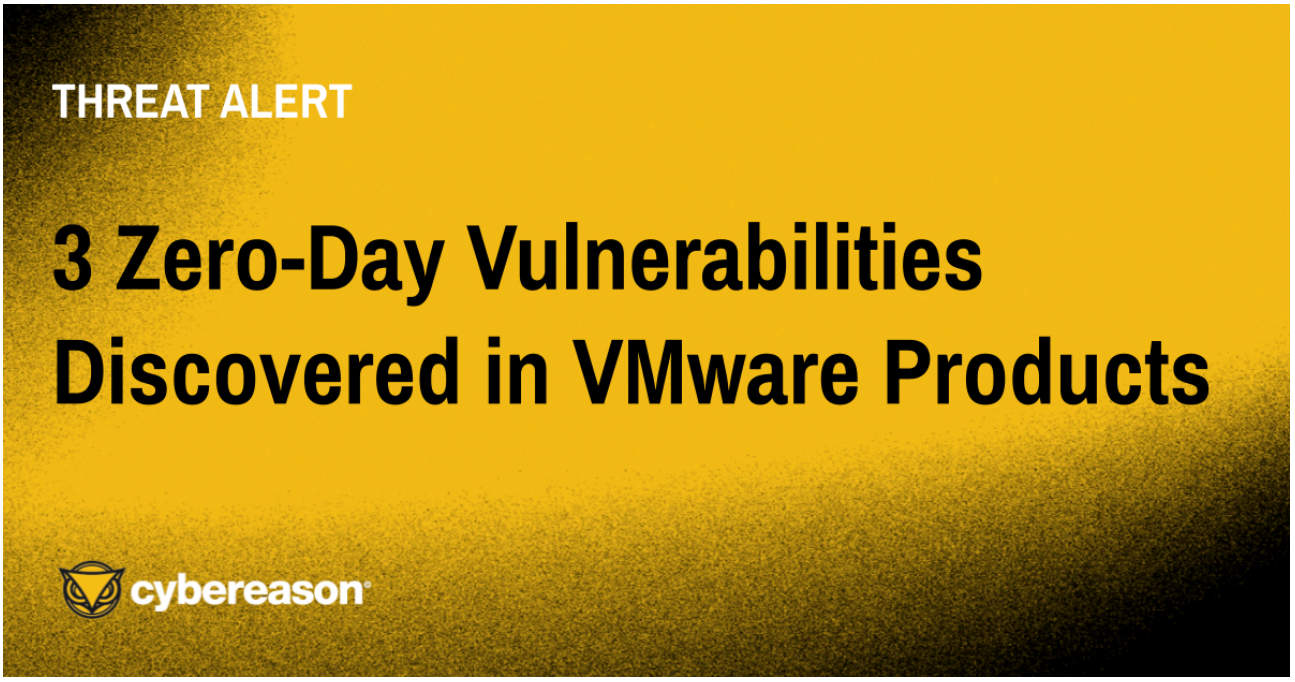
In this Threat Analysis report, Cybereason investigates the PlayBoy Locker, the new Ransomware-as-a-Service, and how to defend against it.

March 25, 2025 / 5 minute read

[Are you keeping pace with Cyber Security AI innovation?]

AI is changing the landscape of detection methodology. In order to stay ahead of adversaries, Greg Day breaks down how cybersecurity vendors need leverage AI within their threat detection, prevention & response.

March 17, 2025 / 5 minute read




BLOG
Deceptive Signatures:
Advanced Techniques in BEC Attacks
cybereason


BLOG
Enhancing Business Email Compromise Incident Response:
New Email & Cloud Security Configuration Snapshot
cybereason

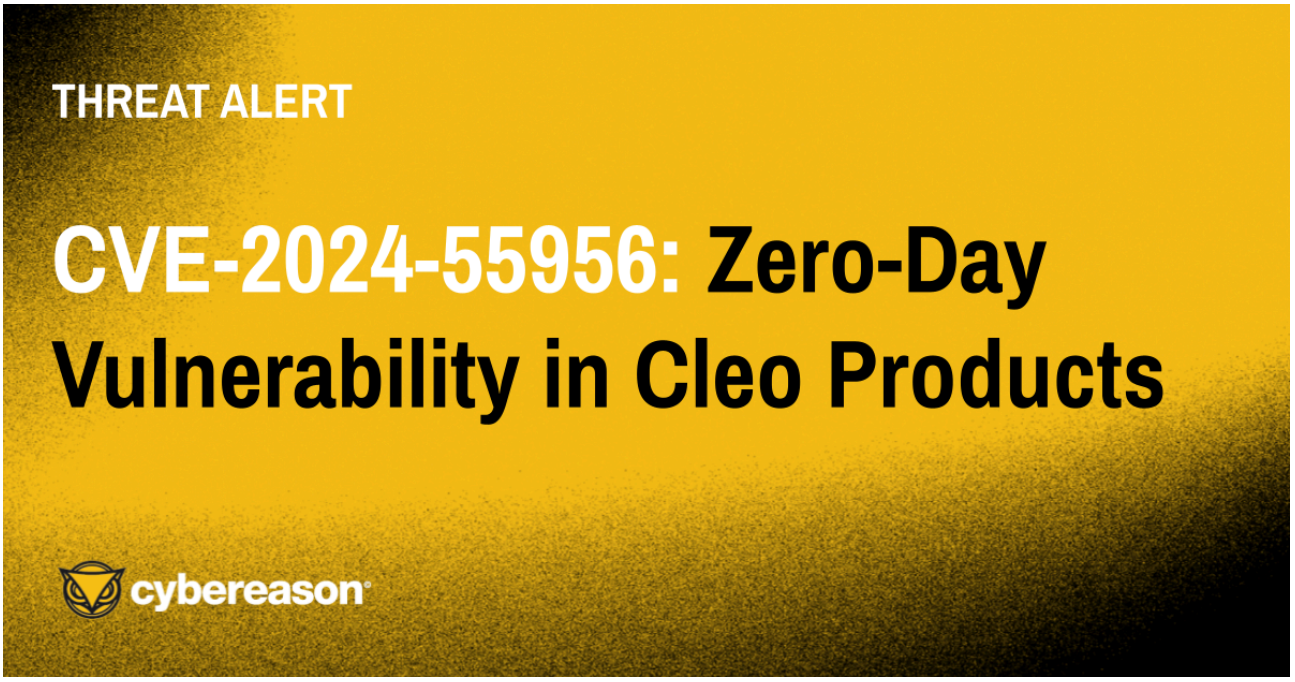

BLOG
RSAC 2025 -
Key Trends from 100s of 'Hackers &
Threats' Talk Submissions
cybereason
RSAC

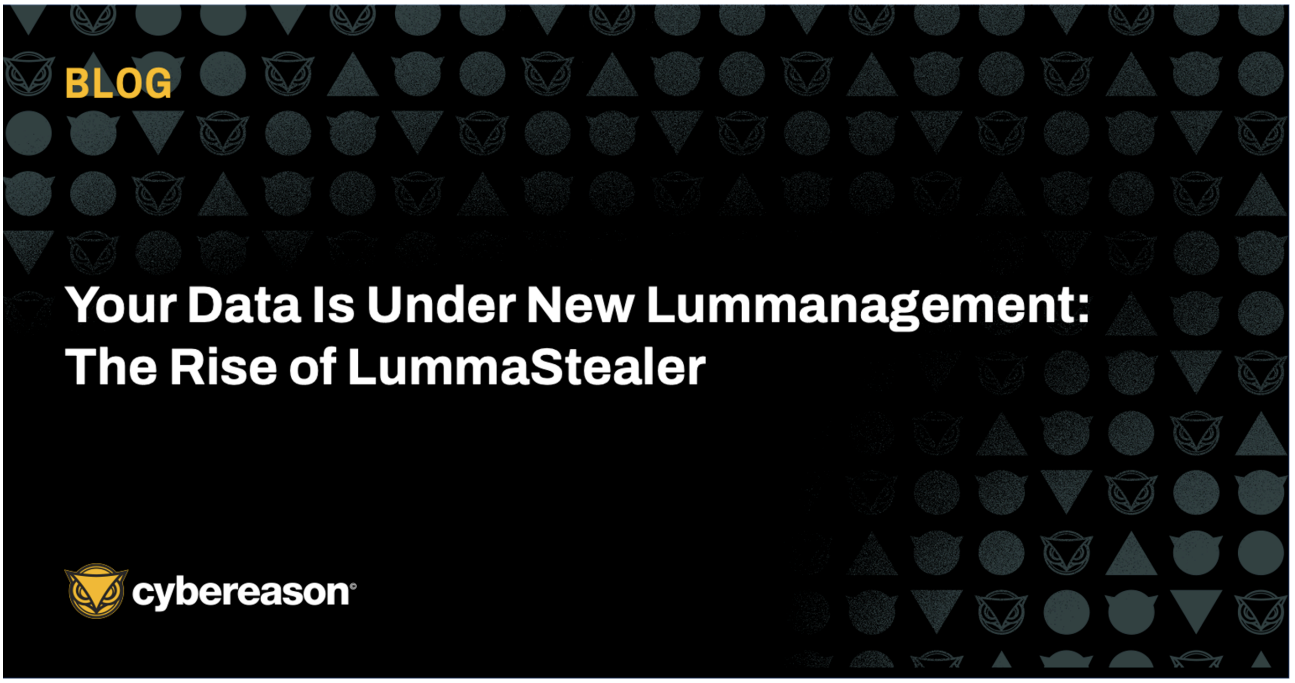

BLOG
Phorpiex - Downloader
Delivering Ransomware
cybereason

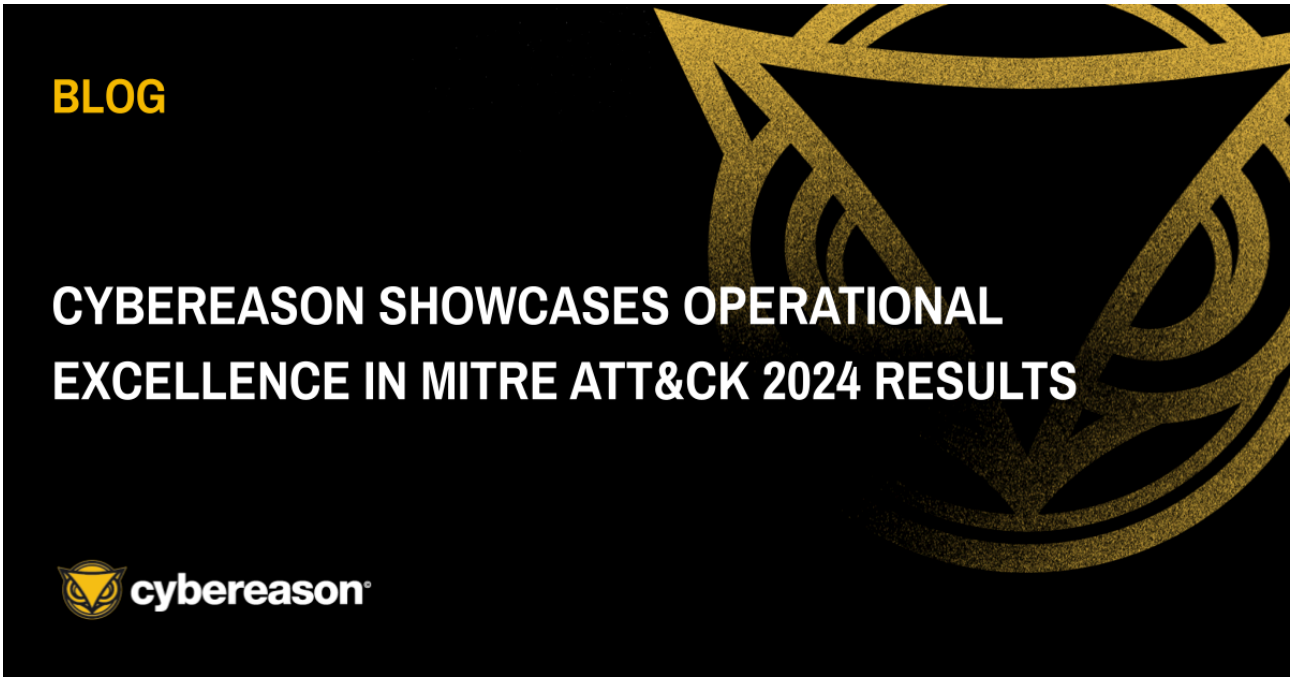

THREAT ALERT
CVE-2025-23006: Critical Vulnerability in SonicWall
cybereason

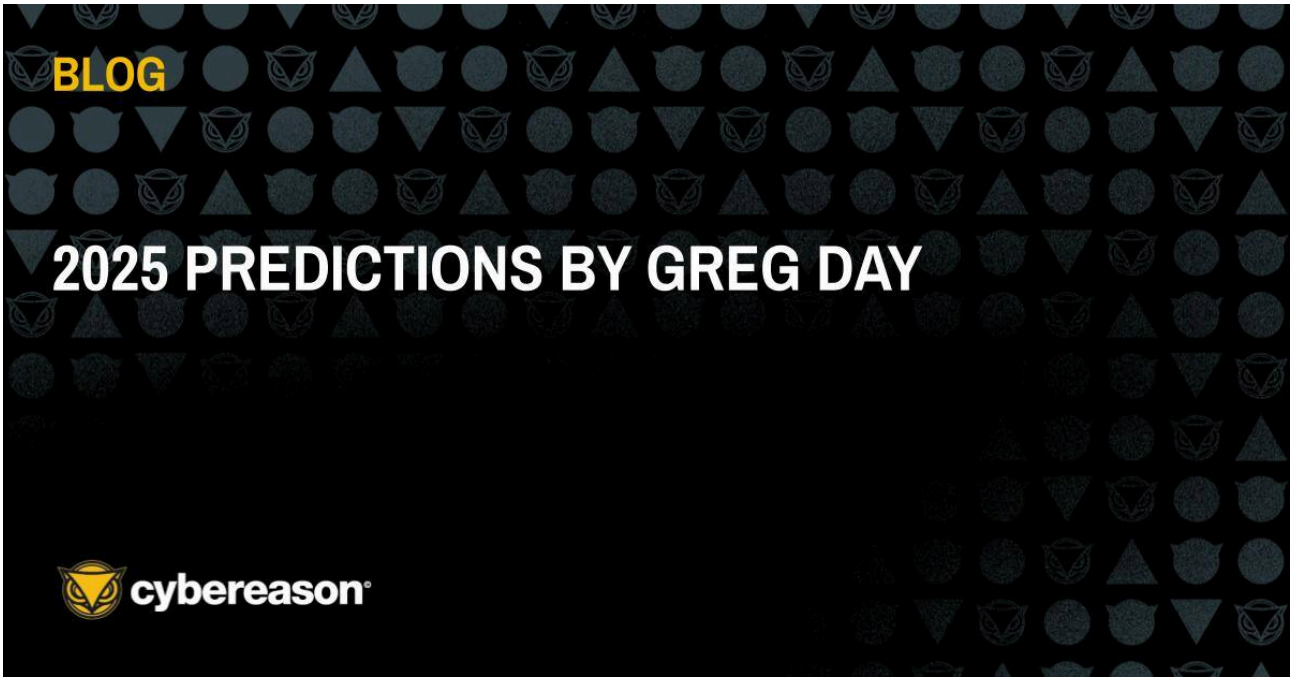

From Noise to Clarity:
The Value of MalOp™ Technology in Modern Cyber Defense


BLOG
"Out-of-the-Box" Detection Coverage:
A Critical Metric for Endpoint Security
cybereason


THREAT ALERT
CVE-2024-55956: Zero-Day
Vulnerability in Cleo Products
cybereason


BLOG
Your Data Is Under New Lummanagement:
The Rise of LummaStealer
cybereason


BLOG
CYBEREASON SHOWCASES OPERATIONAL
EXCELLENCE IN MITRE ATT&CK 2024 RESULTS
cybereason



[2025 Predictions by Greg Day]

At pace, gather enough evidence to understand what was occurring, the first goal being to contain the threat and minimize its impact on the business.

December 11, 2024 / 3 minute read

[Insourcing versus Outsourcing]

what should your own cybersecurity staff do in-house and what should be taken as an outcome based service?

November 8, 2024 / 5 minute read

[Malicious Life Podcast: Operation Snow White, Part 2]

Scientology spies were trained in all covert operations techniques: surveillance, recruiting agents, infiltrating enemy lines, and blackmail. However, a suspicious librarian and a determined FBI agent brought the largest single spy operation in US government history to an end.

October 23, 2024 /

[THREAT ANALYSIS: Beast Ransomware]

In this Threat Analysis report, Cybereason investigates the Ransomware-as-a-Service (RaaS) known as Beast and how to defend against it through the Cybereason Defense Platform.

October 18, 2024 / 5 minute read

[CUCKOO SPEAR Part 2: Threat Actor Arsenal]

In this report, Cybereason confirms the ties between Cuckoo Spear and APT10 Intrusion Set by tying multiple incidents together and disclosing new information about this group's new arsenal and techniques.

October 4, 2024 / 13 minute read

[Malicious Life Podcast: Operation Snow White, Part 1]

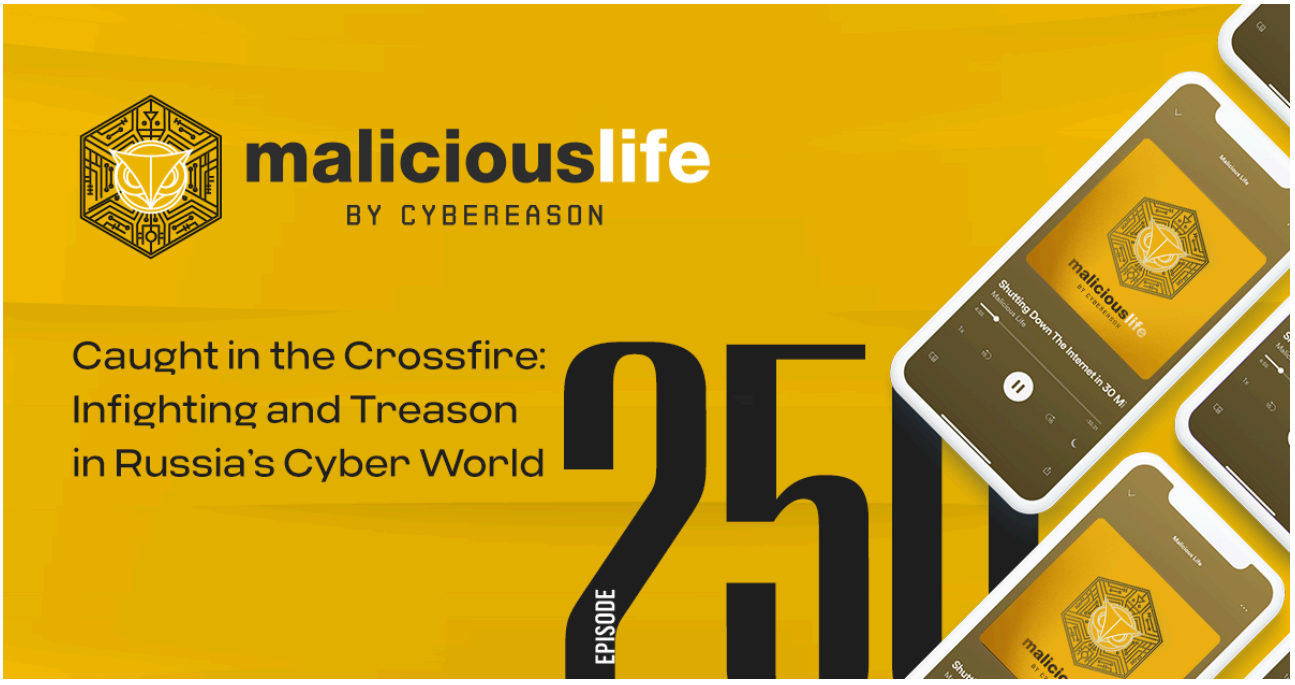
In 1963, the FDA raided the headquarters of a budding new and esoteric religion - The Church of Scientology. In response to this and similar incidents to come, the church's founder - an eccentric science fiction author named L. Ron Hubbard - would go on to lead the single largest known government infiltration operation in United States history.

October 1, 2024 /

[The Great Debate: On-Premise vs. Cloud based EDR]

Should businesses prioritize cloud-based or on-premise cybersecurity solutions, or are CIOs being influenced by a variety of strategic factors and opting for a hybrid approach?

September 18, 2024 / 7 minute read



[Malicious Life Podcast: Infighting and Treason in Russia's Cyber World]

On Dec. 5, 2016, two senior Russian Intelligence officers and two civilians were arrested and accused of treason. A few weeks later, when Western journalists were finally able to speak with the men's lawyers, they learned that the case was based on events that were, oddly enough, already widely known. This made the arrests even more peculiar.

September 17, 2024 /


THREAT RESEARCH
CUCKOO SPEAR PART 1: ANALYZING NOOPDOOR FROM AN IR PERSPECTIVE
cybereason


BLOG
SOC MODERNIZATION: WHERE ARE YOU ON THE EVOLUTIONARY JOURNEY?
cybereason

[Malicious Life Podcast: SNAP Fraud: Getting Rich by Stealing from the Poor]

SNAP - better known as food stamps - goes back to the Great Depression. The physical stamps were replaced with EBT cards in the 1990s, but since these cards are without the secure EMV chip technology, enterprising criminals found innovative ways to drain funds meant for low-income families.

September 5, 2024 /

[Malicious Life Podcast: The Hollywood Con Queen, Part 2]

Nicole Kotsianas, an investigator with K2 Intelligence, made it her personal mission to hunt down the Hollywood Con Queen, who cruelly tormented her victims and shattered their dreams. Nicole's efforts bore unexpected fruits,

when she discovered that the Con Queen was actually… a man.

August 27, 2024 /

[Malicious Life Podcast: The Hollywood Con Queen, Part 1]

In 2015, two aspiring script writers flew to Indonesia to meet with executives of a large Chinese film corporation. It was a trap: the Hollywood Con Queen not only coned them out of tens of thousands of dollars, she also cruelly ruined their friendship. Two years later, a corporate investigator working for a big shot Hollywood producer, made a discovery that put her on the trail of this master of deceit.

August 14, 2024 /

[Capability vs. Usability]

Some CISOs I know work on a premise that for every one new technology deployed, two should be removed. I wonder if we tried to apply a similar principle to the operational aspects of cybersecurity, how far we could progress.

August 1, 2024 / 5 minute read

[Malicious Life Podcast: The Doomed Queen's Secret Ciphers]

Discover how George Lasry, a modern codebreaker, uncovered the secrets of Mary, Queen of Scots, hidden in the French National Library for over 400 years. This episode delves into the painstaking process and the historical impact of decoding these ancient messages, revealing the hidden motives and desperate actions of a doomed queen.

July 31, 2024 /

[Malicious Life Podcast: Why Did People Write Viruses In The 80s & 90s?]

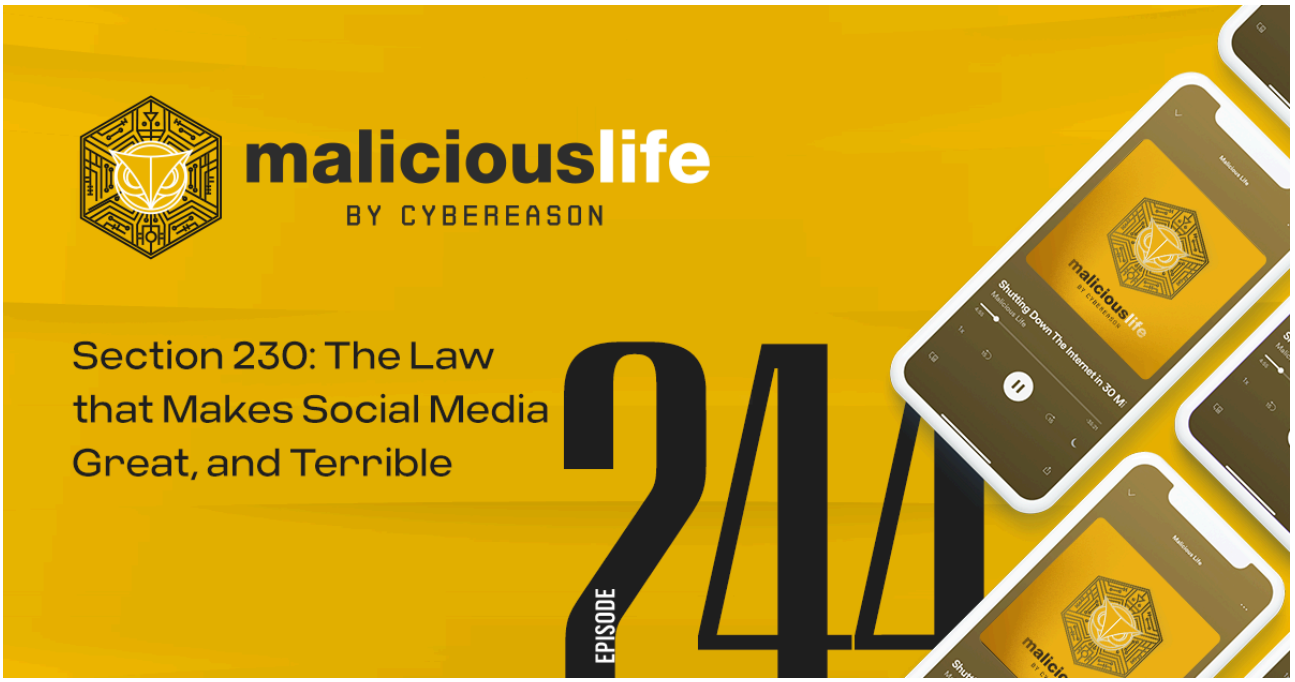
Why did people write malware in the pre-internet days? Back then, there was no way to make money by writing malware. So why write them in the first place? The lack of a financial motivation meant that virus authors had a plethora of other motives - and this diverse mix of motives had, as we shall hear, an interesting effect on the design and style of viruses created at that period.

July 15, 2024 /

[Hardening of HardBit]

In this Threat Analysis report, Cybereason Security Services investigates HardBit Ransomware version 4.0, a new version observed in the wild.

July 10, 2024 / 14 minute read



[Malicious Life Podcast: Section 230: The Law that Makes Social Media Great, and Terrible]

Section 230 is the pivotal law that has enabled the rise of social media -while sparking heated debates over its implications. In this episode, we're charting the history of Section 230, from early landmark legal battles, to

modern controversies, and exploring its complexities and the proposed changes that could redefine online speech and platform responsibility.

June 26, 2024 /

[I am Goot (Loader)]

In this Threat Analysis report, Cybereason Security Services investigate the rising activity of the malware GootLoader. GootLoader is a malware loader known to abuse JavaScript to download post-exploitation malware/tools and persist within the infected machine.

June 25, 2024 / 11 minute read

[Malicious Life Podcast: What Happened at Uber?]

In 2016, Joe Sullivan, former CISO of Facebook, was at the peak of his career. As Uber's new CISO, he and his team had just successfully prevented data from a recent breach from leaking to the internet. But less than a year later, Sullivan was unexpectedly fired from Uber, and three years later, the US Department of Justice announced criminal charges against him. So, what happened at Uber?

June 11, 2024 /

[Malicious Life Podcast: The Nigerian Prince]

In this episode of ML, we're exploring the history of the well-known Nigerian Prince scam, also known as 419 or advanced fee scam, from its roots in a Parisian prison during the French Revolution, to the economic and social reason why this particular scam became so popular with African youth. Also, will AI make such scams more dangerous - or, counter intuitively, go against the interests of scammers?

May 28, 2024 /

[Malicious Life Podcast: Unmasking Secrets: The Rise of Open-Source Intelligence]

Dive into the world of open-source intelligence (OSINT) in this episode, where we uncover how ordinary citizens use publicly available data to unravel some of the most complex global mysteries. From tracking conflicts in real-time to exposing the truth behind high-profile incidents like the downing of Malaysia Airlines flight MH17, discover how OSINT is revolutionizing the field of investigative journalism and transforming how we perceive and verify information.

May 17, 2024 /

[Malicious Life Podcast: The Source Code of Malicious Life]

A few weeks ago we had a listener's meetup in New York, and as part of that meetup, I gave a talk in which I discussed how Malicious Life came to be - a story that goes back to my days as a ship's captain in the Israeli Navy - and then about how me and Nate craft the stories that you hear every other week. That last part, I hope, might also be beneficial to those of you, our listeners, who find themselves giving talks about technically complex ideas, cyber-related or not. The storytelling ideas and techniques I laid out in the talk are universal, and you'll find them in blockbuster movies as well as podcast episodes.

May 1, 2024 /

[Malicious Life Podcast: The Y2K Bug Pt. 2]

In the waning years of the 20th century, amid growing anxieties about the turn of the millennium, one man, Robert Bemer, observed the unfolding drama from his remote home on King Possum Lake. A revered figure in computing, Bemer had early on flagged a significant, looming issue known as the Y2K bug, which threatened to disrupt global systems as calendars rolled over to the year 2000. This episode delves into Bemer's life during this critical period, exploring his predictions, the ensuing global frenzy to avert disaster, and the disparate views on whether the billions spent in prevention were justified or merely a response to a misunderstood threat.

April 23, 2024 /

[Malicious Life Podcast: The Y2K Bug Pt. 1]

In the 1950s and 60s - even leading into the 1990s - the cost of storage was so high, that using a 2-digit field for dates in a software instead of 4-digits could save an organization between $1.2-$2 Million dollars per GB of data. From this perspective, programming computers in the 1950s to record four-digit years would've been outright malpractice. But 40 years later, this shortcut became a ticking time bomb which one man, computer scientist Bob Bemer, was trying to diffuse before it was too late.

April 1, 2024 /

[Threat Alert: The Anydesk Breach Aftermath]

AnyDesk, one of the world’s leading providers of Remote Management and Monitoring (RMM) software, confirmed they had identified a compromise of production systems.

March 22, 2024 / 3 minute read

[Malicious Life Podcast: Can You Bomb a Hacker?]

The 2008 Russo-Georgian War marked a turning point: the first time cyberattacks were used alongside traditional warfare. But what happens when the attackers aren't soldiers, but ordinary citizens? This episode delves into the ethical and legal implications of civilian participation in cyberwarfare, examining real-world examples from Ukraine and beyond.

March 19, 2024 /


BLOG
BEWARE OF THE MESSENGERS, EXPLOITING ACTIVEMQ VULNERABILITY
cybereason


BLOG
BRIDGING THE GAP: BALANCING SECURITY COMPLIANCE AND INNOVATION IN CYBERSECURITY
cybereason

[Malicious Life Podcast: Kevin Mitnick, Part 2]

In 1991, Kevin Mitnick was bouncing back from what was probably the lowest point of his life. He began to rebuild his life: he started working out and lost a hundred pounds, and most importantly - he was finally on the path towards ditching his self-destructive obsession of hacking.

March 1, 2024 /

[Announcing Cybereason On-Prem]

Many of our customers choose Cybereason On-Prem to simplify their data and critical infrastructure compliance with the flexibility to deploy in on-prem server rooms, private data centers or private cloud environments.

February 20, 2024 / 2 minute read

[Malicious Life Podcast: Kevin Mitnick, Part 1]

For Kevin Mitnick - perhaps the greatest social engineer who ever lived - hacking was an obsession: even though it ruined his marriage, landed him in scary correction facilities and almost cost him his sanity in solitary

confinement, Mitnick wasn't able to shake the disease that compelled him to keep breaking into more and more communication systems.

February 19, 2024 /

[THREAT ALERT: Ivanti Connect Secure VPN Zero-Day Exploitation]

Cybereason issues Threat Alerts to inform customers of emerging impacting threats, including critical vulnerabilities such as the Ivanti Connect Secure VPN Zero-Day exploitation. Cybereason Threat Alerts summarize these threats and provide practical recommendations for protecting against them.

February 6, 2024 / 9 minute read

[Malicious Life Podcast: SIM Registration: Security, or Surveillance?]

Right now, hundreds of thousands of people in the southern African country of Namibia are faced with a choice. At the end of next month, their phone service is going to be shut off permanently: to prevent that from happening, they'll have to give up their data privacy. As a result, nearly two million Namibian citizens are facing a data privacy problem which may haunt them for years to come - and hundreds of thousands more are set to join them, or else they'll lose their phone service for good. All of which raises the question: was making everybody register their SIM cards a good idea in the first place?

February 5, 2024 /

[THREAT ALERT: DarkGate Loader]

The execution of DarkGate Loader ultimately leads to execution of post-exploitation tools such as Cobalt Strike and Meterpreter. This Threat Alert provides an overview of an attack involving DarkGate Loader.

January 29, 2024 / 2 minute read

[Malicious Life Podcast: The Mariposa Botnet]

In 2008, The 12 million PCs strong Mariposa Botnet infected almost half of Fortune 100 company - but the three men who ran it were basically script kiddies who didn't even knew how to code.

January 22, 2024 /

[What's on the Smartest Cybersecurity Minds for 2024?]

I had the huge privilege of being on the program committee for the RSA Conference 2024, reviewing the always popular track: Hackers and Threats, which were a great indicator of the challenges we should expect to see in the coming year.

January 16, 2024 / 3 minute read

[Malicious Life Podcast: The Real Story of Citibank's $10M Hack]

Valdimir Levin is often presented as "the first online bank robber," and appeares on many lists of the "Top 10 Greatest Hackers." But a few veteran Russian hackers cliam that Levin's infamous hack had been mangled by the

journlists who wrote about it. What's the truth behind the 1994 $10.7 million Citibank hack?…

January 9, 2024 /

[Malicious Life Podcast: How to Hack Into Satellites]

About a year ago, six academics from Ruhr University Bochum and the CISPA Helmholtz Center for Information Security set out to survey engineers and developers on the subject of satellite cybersecurity. But most of these engineers were very reluctant to share any details about their satellites and their security aspects. Why were satellite engineers so reticent to talk about cybersecurity? What was so secretive, so wrong with it, that they didn’t feel they could answer even general questions, anonymously? Because let’s be clear: if there’s something wrong with the security of satellites, that’d be a serious problem.

December 27, 2023 /

[THREAT ALERT: CITRIXBLEED (CVE-2023-4966)]

Cybereason issues Threat Alerts to inform customers of emerging threats, including critical vulnerabilities such as CitrixBleed. Cybereason Threat Alerts summarize these threats and provide practical recommendations for protecting against them.

December 18, 2023 / 3 minute read

[Malicious Life Podcast: Moonlight Maze]

When investigators discovered in 1996 that US military networks were being extensively hacked, they didn't realize they were witnessing the birth of what would become Russia's formidable Turla APT espionage group. We

uncover the 20-year metamorphosis of this original group of hackers into one of the most sophisticated and dangerous state-sponsored threats that's still active today.

December 11, 2023 /

[Malicious Life Podcast: Volt Typhoon]

In August 2021, a port in Houston, Texas, was attacked. Over the following months, a series of attacks occurred in various locations, reminiscent of a serial killer's pattern. Targets included telecommunications companies, government agencies, power plants, and water treatment facilities. How did Volt Typhoon manage to evade authorities and analysts for such an extended period?

November 28, 2023 /


BLOG
THREAT ALERT: DJVU VARIANT DELIVERED BY LOADER MASQUERADING AS FREEWARE
cybereason


BLOG
2024 CYBERSECURITY PREDICTIONS: GENERATIVE AI RESHAPES CYBERSECURITY
cybereason

[THREAT ALERT: INC Ransomware]

Cybereason issues Threat Alerts to inform customers of emerging impacting threats, including new ransomware actors such as the emergent group INC Ransom. Cybereason Threat Alerts summarize these threats and provide practical recommendations for protecting against them.

November 20, 2023 / 3 minute read

[Malicious Life Podcast: Is NSO Evil? Part 2]

By the time Forbidden Stories published its “Pegasus Project” in 2021, NSO was already knee deep in what was probably the worst PR disaster ever suffered by a cybersecurity company - and then, in November 2021, came the

fateful blow: the US Dept. of Commerce added NSO to its “Entity List.” Is NSO to blame for its troubles? Could the company have acted differently to prevent its downfall?

November 13, 2023 /

[Malicious Life Podcast: Is NSO Evil? Part 1]

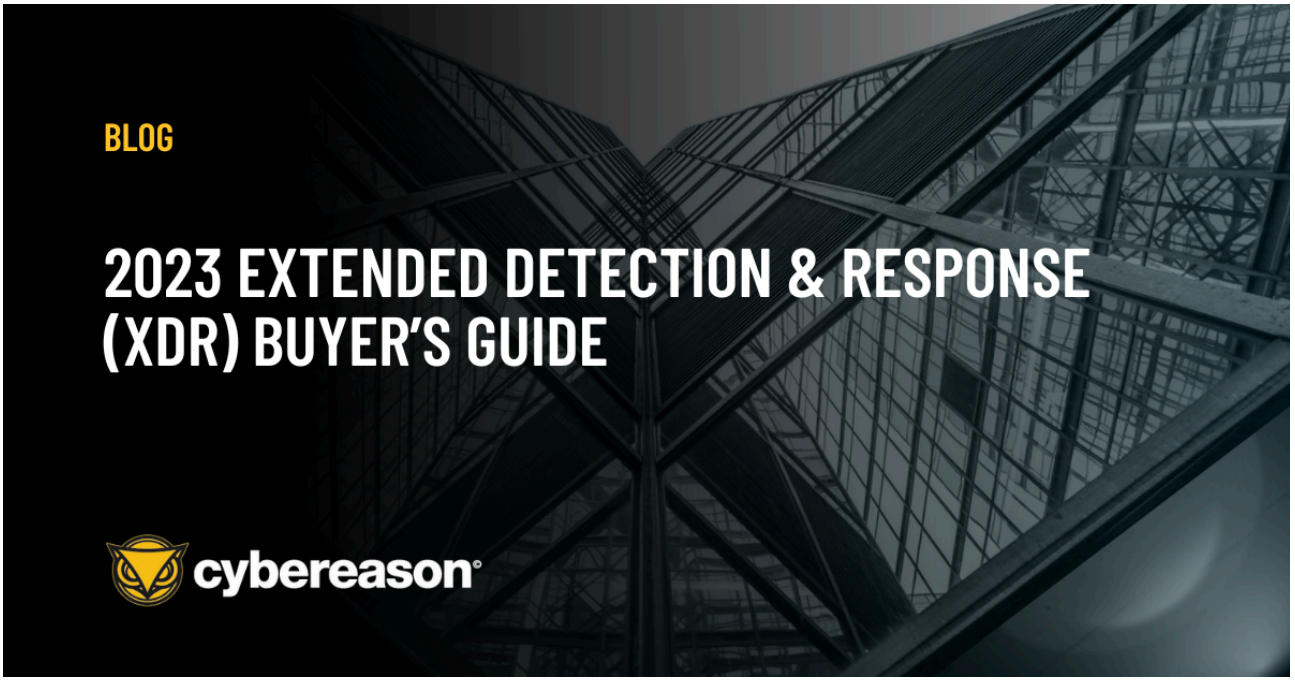
NSO Group, creator of the infamous Pegasus spyware, is widely regarded as a vile, immoral company: a sort of 21st century soldier of fortune, a mercenary in the service of corrupt and evil regimes. Yet among its many clients are many liberal democracies, including the US, Germany, the Netherlands and Spain, to name but a few. So, is NSO really as evil as many think it is?

October 30, 2023 /

[EU Network Information Security]

It's not surprising that in the last couple of months the requests of “are you EU Network Information Security Directive (NISD) v2 compliant?” are starting to come in. What would seem like a simple GRC yes no question is in fact complex.

October 25, 2023 / 3 minute read

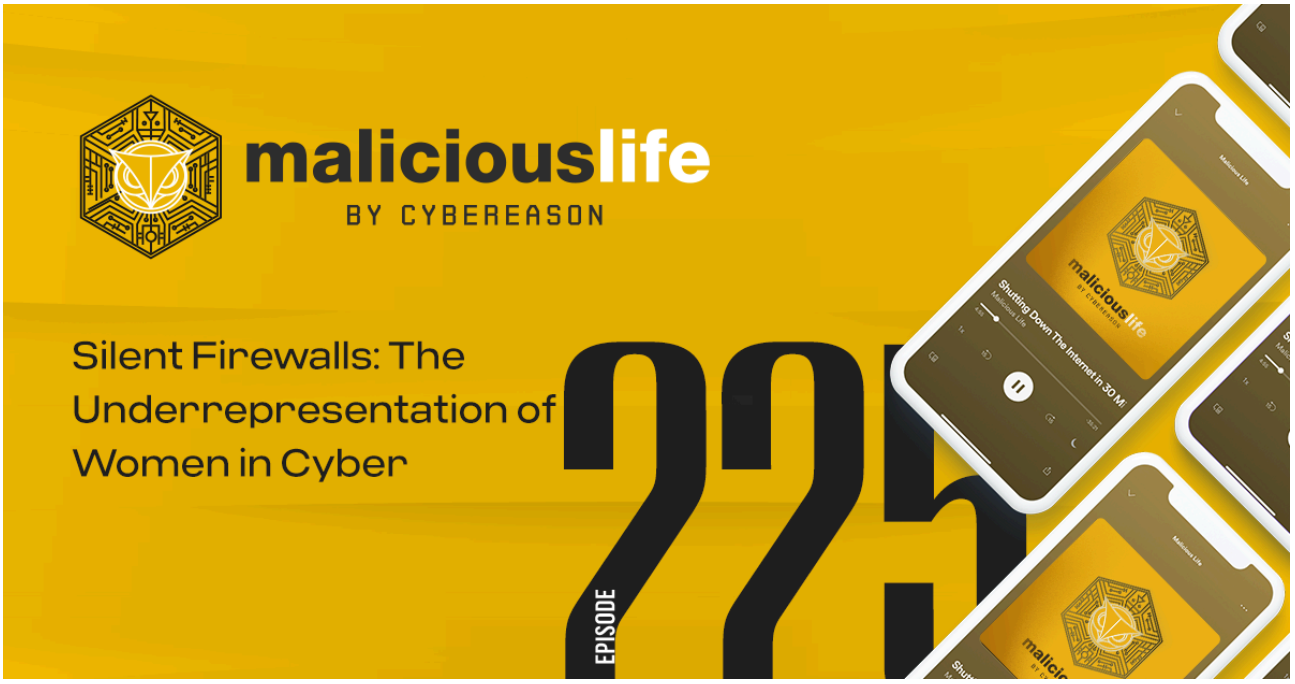


[2023 Extended Detection & Response (XDR) Buyer’s Guide]

To support cyber defenders to achieve tangible business benefits and deliver effective security outcomes, Cybereason has developed a comprehensive Extended Detection & Response (XDR) Buyer’s Guide.

October 24, 2023 / 1 minute read


BLOG
THREAT ANALYSIS: TAKING SHORTCUTS... USING LNK FILES FOR INITIAL INFECTION AND PERSISTENCE
cybereason


maliciouslife
BY CYBEREASON
Silent Firewalls: The Underrepresentation of Women in Cyber
EPISODE 223

[Malicious Life Podcast: Operation Kudo]

In 1981, during the G7 Summit in Quebec, French president Francois Mitterand handed President Raegan a top secret collection of documents, called Farewell Dossier. The information found in the dossier allowed the US to devise a cunning plan - the very first supply chain attack, if you will - to bring a firey end to one of largest industrial espionage campaigns in history.

September 20, 2023 /

[The Cybersecurity Capability the Industry Nearly Forgot]

How do we secure the Private Infrastructure Protection (PIP) space? By providing virtualized containers, allowing customers to re-use their own hardware and making it easier to add in new capabilities as the cyber security world evolves.

September 13, 2023 / 4 minute read

[Malicious Life Podcast: Can We Stop the AI Cyber Threat?]

Much of the cybersecurity software in use today utilizes AI, especially things like spam filters and network traffic monitors. But will all those tools be enough to stop the proliferation of malware that will come from generative

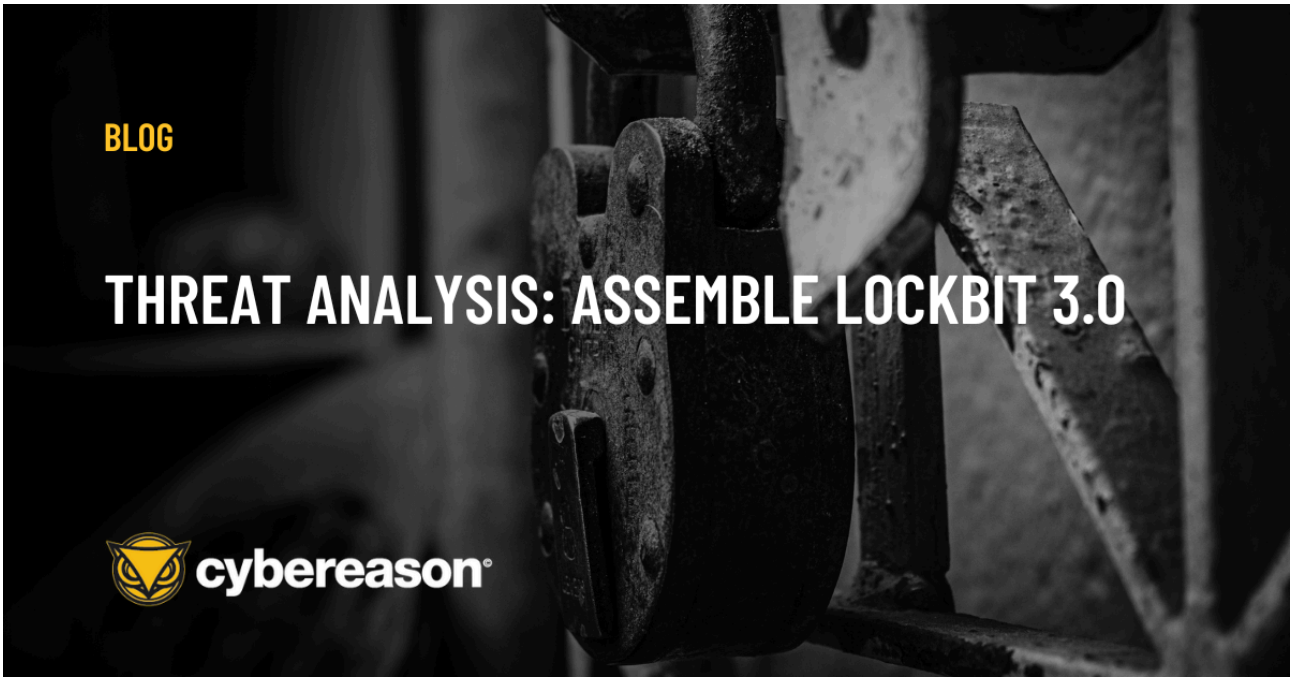
AI-driven cyber attacks? The potential of AI to disrupt cyberspace is far greater than any solutions we've come up with thus far, which is why some researchers are looking beyond the traditional answers, towards more aggressive measures.

September 4, 2023 /

[Malicious Life Podcast: Is Generative AI Dangerous?]

Every so often, the entire landscape of cybersecurity shifts, all at once: The latest seismic shift in the field occurred just last year. So in this episode of Malicious Life we're going to take a look into the future of cybersecurity: at how generative AI like ChatGPT will change cyberspace, through the eyes of five research teams breaking ground in the field. We'll start off simple, and gradually build to increasingly more complex, more futuristic examples of how this technology might well turn against us, forcing us to solve problems we'd never considered before. – check it out...

August 22, 2023 /



[THREAT ANALYSIS: Assemble LockBit 3.0]

LockBit 2.0 ransomware attackers are constantly evolving and making detection, investigation, and prevention more complex by disabling EDR and other security products and deleting the evidence to stifle forensics attempts...

August 21, 2023 / 4 minute read

[Malicious Life Podcast: Why aren't there more bug bounty programs?]

On the face of it, there's an obvious economic incentive for both vendors and security researchers to collaborate on disclosing vulnerabilities safely and privately. Yet bug bounty programs have gained prominence only in the past decade or so, and even today only a relatively small portion of vendors have such programs at place. Why is that? – check it out...

August 8, 2023 /

[Malicious Life Podcast: The Voynich Manuscript]

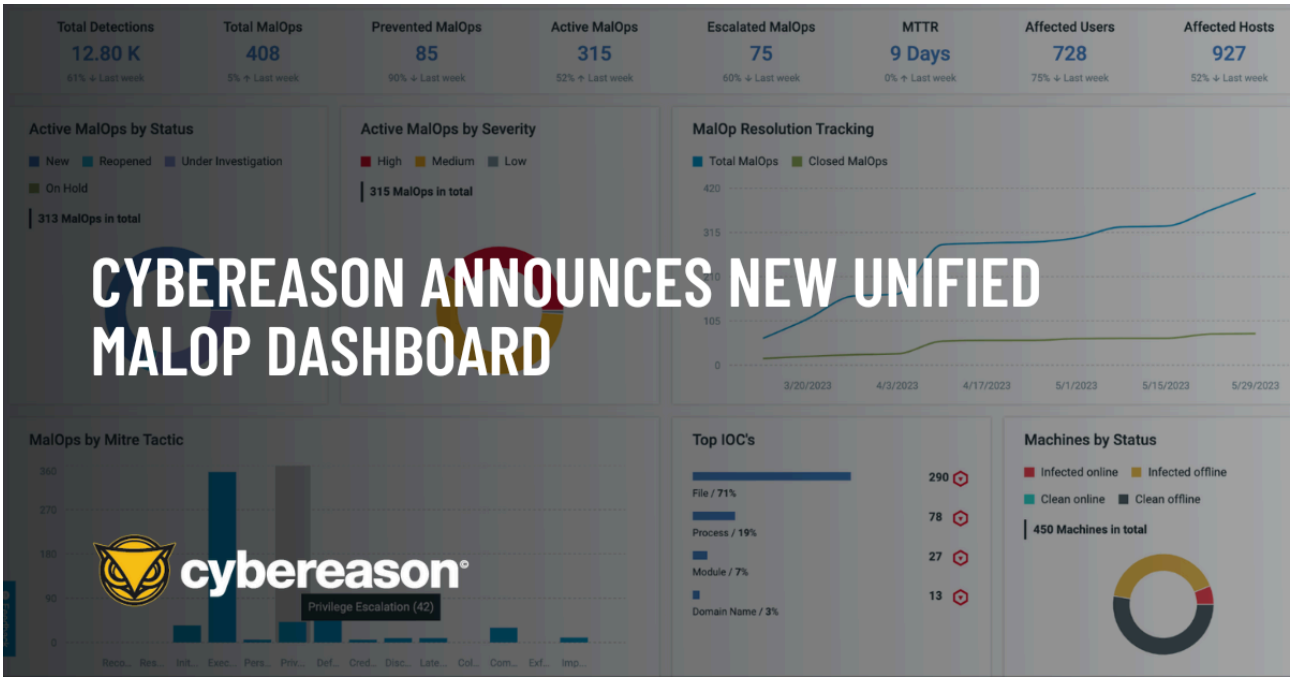
The constant battle between those who wish to encrypt data and those who wish to break these ciphers has made modern encryption schemes extremely powerful. Subsequently, the tools and methods to break them became equivalently sophisticated. Yet, could it be that someone in the 15th century created a cipher that even today's most brilliant codebreakers and most sophisticated and advanced tools - cannot break?...

July 25, 2023 /

[Malicious Life Podcast: Roman Seleznev: Did the Punishment Fit the Crime?]

In 2019, Roman Seleznev, a 34 years-old Russian national, was sentenced to 27 years in prison: A sentence that'd make any criminal quiver. Seleznev's deeds had a horrendous effect on the 2.9 million individuals whose credit cards he stole and sold to cyber criminals for identity theft and financial crimes. On one hand, it's hard to imagine any nonviolent computer crime worth 27 years in prison. But then what is an appropriate sentence for such a man as Seleznev? – check it out...

July 10, 2023 /



Cybereason's New Unified MalOp Dashboard

To help SOC teams stay ahead of the curve, Cybereason introduced a unified dashboard designed to provide additional insights into emerging threats, operational metrics and provide insights to continuously improve SOC processes and procedures.

July 7, 2023 / 2 minute read

Malicious Life Podcast: Sony BMG's Rootkit Fiasco

"We made a mistake and Sony paid a terrible price.” A terrible price indeed: an arrogant and ill-advised decision to include a rootkit in its music CDs cost Sony BMG a lot of money - and painted it as a self-centered, self-serving

company that cares more about its bottom line than its customers. Why did Sony BMG make such a poor decision? – check it out...

June 27, 2023 /

[Malicious Life Podcast: Ad Fraud, Part 2]

"What makes ad fraud so successful, and so prevalent, and why can't we stop it? The answer isn't technical at all. It's not hard to understand. But it's a harsh reality that many people are simply not willing to face. – check it out...

June 9, 2023 /

[Malicious Life Podcast: Ad Fraud, Part 1]

Right now, a man named Aleksandr Zhukov is sitting in jail for one of the most financially ruinous schemes ever invented for the internet. Zhukov is guilty. He was caught and convicted under a mountain of evidence against him. Except the deeper you look into it, the deeper the well goes. In this episode, we'll learn how Aleksandr Zhukov defrauded some of the biggest American corporations for millions of dollars. And we'll ask the question that hardly anyone else is willing to acknowledge: Was this clever, successful, guilty cybercriminal merely a fall guy for everybody else playing his twisted game?. – check it out...

May 30, 2023 /

[Malicious Life Podcast: The Economics Of Cybersecurity]

The numbers can't be any clearer: a DDoS attack costs less than a hundred dollars, while the price tag for mitigating it might reach tens if not hundreds of thousands of dollars. A single well crafted phishing email can easily circumvent cyber defenses which cost millions of dollars to set up. How can we change the extreame cost asymmetry between attackers and defenders in cyberspace?. – check it out...

May 15, 2023 /

[Malicious Life Podcast: The Reason You Don't Have Data Privacy]

We've all experienced the creepiness of modern data trafficking, but that kind of daily annoyance is the surface of a much bigger issue: Big Tech companies such as Amazon & Microsoft are lobbying policymakers to veto laws that harm their business, and often hide their lobbying behind industry coalitions or organizations with names that are vague and seemingly harmless. Will current and future privacy laws actually protect your information, or will they protect the companies collecting your information? – check it out...

May 1, 2023 /

[Malicious Life Podcast: How Entire Countries Can Lose the Internet]

Disruptions to the world's internet cables happen more often than you think: Whether it be ship anchors or animals or saboteurs, cut a few wires in the right places and at nearly the speed of light you can disrupt or shut off the internet for broad populations of people at a time. It is an immense power that runs through these lines -- a power that can be sabotaged or, in the right hands, weaponized. – check it out...

April 17, 2023 /

[Malicious Life Podcast: Olympic Destroyer]

In the midst of 35,000 exhilarated spectators eagerly chanting the time-honored countdown to kick off the 2018 Pyeongchang Winter Olympics, a sinister malware crept through the games' network, threatening to disrupt the highly-anticipated event. The obvious question in everyone’s minds was - who was responsible for the attack? Who was vile enough to launch such a potentially destructive attack against an event which, more than anything, symbolizes peace and global cooperation? – check it out...

April 3, 2023 /

[Malicious Life Podcast: The Lawerence Berkeley Hack, Part 2]

On May 23rd, 1989, Karl Koch - a 23 years old West German hacker who worked for the KGB - took a drive, from which he would never return: Nine days later his charred remains were found by the police in a remote forest. Was Koch assasinated by the US or the Sovient Union, or is there another, more 'mystical' explanation for his death? – check it out...

March 20, 2023 /

[5 Steps to More Effective Ransomware Response]

Investing in technology can give companies a false sense of security when it comes to ransomware. Here are 5 steps to more effective ransomware response.

March 15, 2023 / 3 minute read

[Malicious Life Podcast: The Lawerence Berkeley Hack, Part 1]

Four decades ago, three quarters would've gone a lot further than they do today. With that kind of loose change you could've picked up some milk from the grocery store, or over half a gallon of gas, or a bus ticket. But that doesn't explain why, on one fateful day in 1986, a systems administrator at the Lawrence Berkeley National Laboratory in California made such an issue over 75 missing cents. – check it out...

March 8, 2023 /

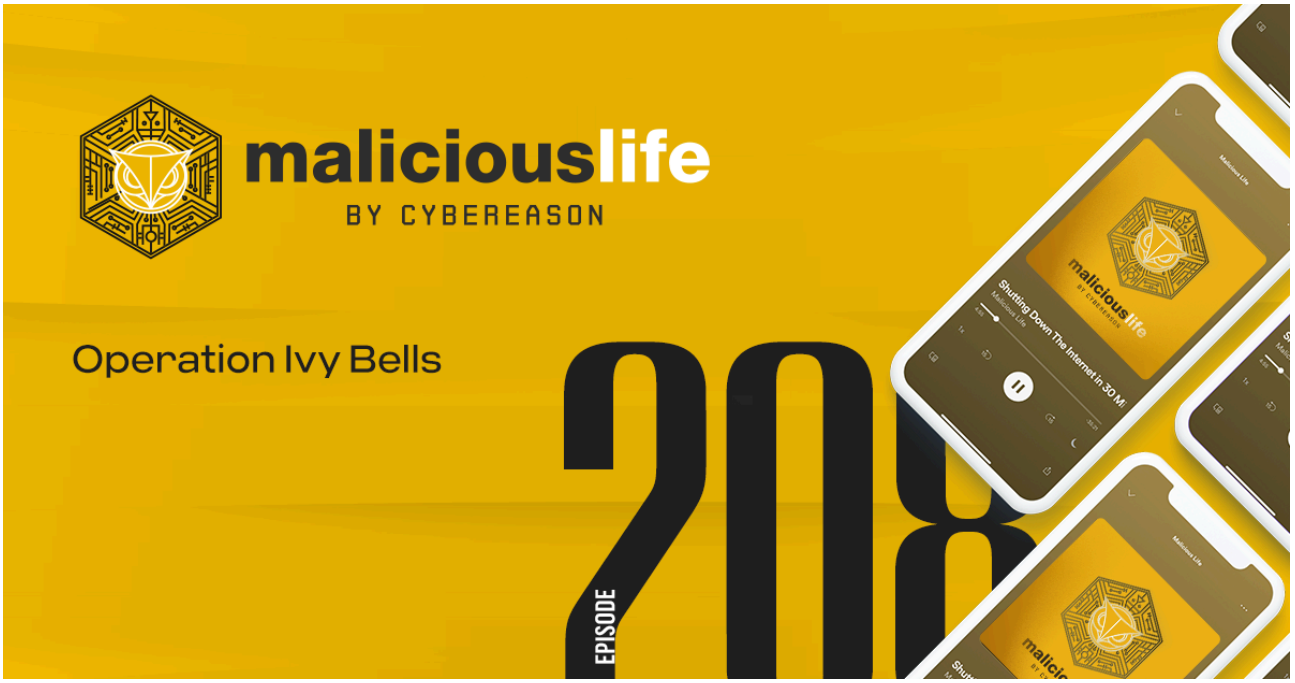
[Malicious Life Podcast: Russian Propaganda, Explained [ML B-Side]]

In this B-Side episode, our Senior Producer Nate Nelson interviewed Dr. Bilyana Lilly - CISSP, a leader in cybersecurity and information warfare with over fifteen years of managerial, technical, and research experience, and author of "Russian Information Warfare" - about the Russian use of instant messaging and social media platforms such as Telegram and Twitter in their war efforts. Dr. Lilly discusses who they are targeting and the real-world impact their propaganda has on various populations. – check it out...

February 28, 2023 /


BLOG
Cybereason Named a Leader in 2022 Gartner® Magic™ Quadrant for Endpoint Protection Platforms
cybereason


BLOG
New Studies Paint Bleak Picture of Future SOC Effectiveness
cybereason



[Malicious Life Podcast: Operation Ivy Bells]

In the early 1970's, US intelligence pointed at the possibility that the Russians have laid an underwater communication cable between two important naval bases in the Far East. The dangerous mission of installing a listening device on that cable was given to the navy most secretive and unusual submarine. – check it out...

February 20, 2023 /

[Ransomware Shifting to the Cloud]

We are already seeing ransomware that scans for cloud-based collaboration points. And while you may think the risks are the same, that's not the case.

February 14, 2023 / 4 minute read

[Malicious Life Podcast: Why Do NFTs Disappear? [ML BSide]]

What happens when an NFT marketplace goes under, and disappears? You would imagine that the users' NFTs are perfectly safe: after all, the blockchain itself is still there, right? But that's not how things work in the real world.

February 13, 2023 /

[Malicious Life Podcast: The (Other) Problem with NFTs]

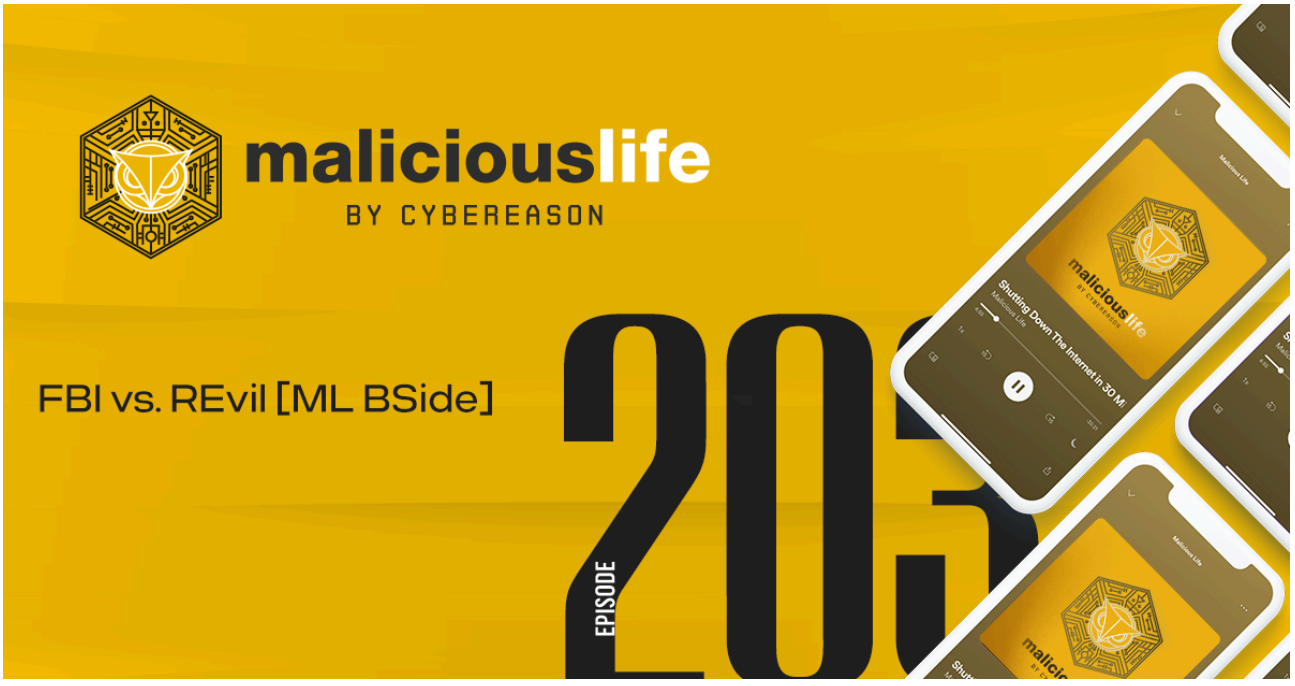
Financial markets make good targets for criminals - after all, that's where the big money is. Surprisingly, many of these criminals are not your run-of-the-mill black hat hacker, but brokers registered with the SEC: genuine finance industry professionals – check it out...

February 6, 2023 /

[You Should Be Afraid of SIM Swaps]

If SIM swap stories ever make the news, almost uniformly, they focus on people who lost a lot of money. But SIM swaps also take a psychological toll...

January 31, 2023 /



[FBI vs. REvil [ML BSide]]

Nate Nelson speaks with Rich Murray, who leads the FBI's North Texas Cyber unit, about how the Federal Bureau of Investigations dealt with dealt with another attack by REvil

January 24, 2023 /

[Cyberbunker, Part 2]

Spamhaus's decision to add Cyberbunker to its list of Spam sources led the Stophaus coalition to initiate a DDoS attack later dubbed “The attack that almost broke the Internet.”

January 20, 2023 /

[7 Requirements for a Successful XDR Strategy]

If you’re a security practitioner wondering where to start your XDR journey, here’s a look at the fundamental building blocks of a successful XDR strategy.

January 19, 2023 / 3 minute read

[Cyberbunker, Part 1]

Sven Kamphuis and Herman Johan Xennt are quite dissimilar... and in 1996, their unlikely partnership coalesced around a mutual deep hatred towards authority...

January 11, 2023 /

[How Netflix Learned Cloud Security [ML B-Side]]

2011 was a pivotal year for Netflix: the now hugely successful company was then in the midst of a formidable transformation, changing from a mail-based DVD rental service to the modern streaming service that it is today

January 3, 2023 /

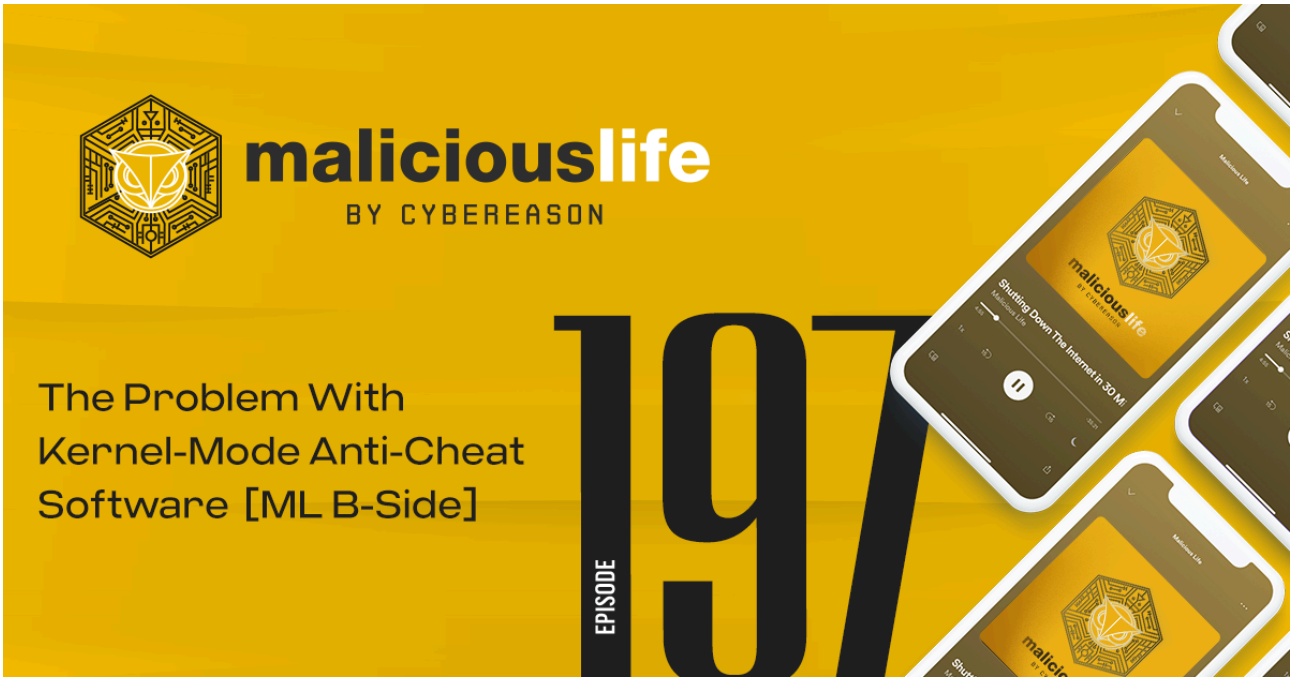
[Royal Rumble: Analysis of Royal Ransomware]

Royal ransomware has become one of the most prolific ransomware groups in 2022. Read our threat analysis to learn how Royal ransomware operations work, how they evade anti-ransomware defenses, and how you can outsmart them.

December 14, 2022 / 7 minute read


BLOG
Case Study: How Cybereason MDR Improved Olist's Triage & Response Time
cybereason


maliciouslife
BY CYBEREASON
Thamar Reservoir
EPISODE
198



[The Problem With Kernel-Mode Anti-Cheat Software [ML B-Side]]

Nobody likes cheaters, especially in video games. That's why EA and other publishers are implementing kernel-mode anti-cheat software in their games. Yet some people warn that installing such kernel-level systems is extremely dangerous. In this episode of Malicious Life, we examine why.

December 8, 2022 /

[Threat Analysis: MSI - Masquerading as a Software Installer]

Learn how threat actors are embedding malicious binaries and scripts in legitimate Microsoft Windows Installation (.msi) files to take over machines they're targeting with elevated privileges. Find out how to detect this sophisticated attack technique.

December 5, 2022 / 16 minute read

[FBI, CISA Issue Warning on Cuba Ransomware]

The FBI and CISA issued a joint advisory on Cuba ransomware actors. The advisory is the latest in the government's #StopRansomware campaign.

December 2, 2022 / 2 minute read

[Nine Cybersecurity Predictions for 2023]

Cybereason VP and EMEA Field CISO Greg Day anticipates 2023 will bring more cloud credential attacks, increased use of deepfakes in blended attacks, attacks between smart devices, and more.

December 1, 2022 / 3 minute read

[The Russian Business Network]

Find out how the Russian Business Network, a once legitimate ISP, became the largest player in the Russian cybercrime world and a key component of Putin's attacks on democracy and misinformation campaigns in this episode of the Malicious Life podcast.

November 25, 2022 /

[What Can Chess Grandmasters Teach Us About Cyber]

Find out what cybersecurity professionals can learn from MMA wrestlers and Chess Grand Champions about peak performance in this episode of Malicious Life, featuring Chris Cochran and Ron Eddings, the co-founders of

Hacker Valley Media.

November 24, 2022 /

[Malicious Life Podcast: LabMD vs. The FTC]

One day in 2008, Michael Daugherty got a call from cybersecurity company TiVera, saying private medical data of some 9000 LabMD patients had been discovered online. When Michael refused to pay for TiVersa's hefty "consultation fee", a ten-year legal battle began that led to the demise of LabMD, but also cost the FTC dearly.

November 18, 2022 /


BLOG
NGAV Redefined: 9 Layers of Unparalleled Attack Protection
cybereason


BLOG
Machine Timeline Enhancements Improve Investigation Workflows
cybereason

[THREAT ANALYSIS REPORT: DLL Side-Loading Widely (Ab)Used]

This Threat Analysis Report explores widely used DLL Side-Loading attack techniques, outlines how threat actors leverage these techniques, describes how to reproduce an attack, and reports on how defenders can detect and prevent these attacks...

October 26, 2022 / 13 minute read

[Operationalizing MITRE ATT&CK: A New Wave is Here]

The Tidal Platform makes it efficient to research adversary techniques using MITRE ATT&CK, and now Cybereason has joined the Tidal Product Registry to deliver a visual view of our out-of-the-box detection

capabilities...

October 19, 2022 / 2 minute read

[Malicious Life Podcast: Hacking Stock Markets Part 2]

Financial markets make good targets for criminals - after all, that's where the big money is. Surprisingly, many of these criminals are not your run-of-the-mill black hat hacker, but brokers registered with the SEC: genuine finance industry professionals – check it out...

October 18, 2022 /

[Indicators of Behavior and the Diminishing Value of IOCs]

IOBs describe the subtle chains of malicious activity derived from correlating enriched telemetry from across all network assets - but unlike backward-looking IOCs, IOBs offer a proactive means to leverage real-time telemetry to identify attack activity earlier, and they offer more longevity value than IOCs...

October 12, 2022 / 4 minute read

[Why NGAV Displaced Traditional Antivirus Tools]

NGAV can work to prevent the early stages of a ransomware attack that precede the delivery of the ransomware payload, and offers further protection by also assuring that payload is not detonated on the target machine in the

case where the first stages of the attack were not detected...

October 11, 2022 / 4 minute read

[Malicious Life Podcast: Vishing Voice Scams]

Rachel Tobac is a hacker and CEO of SocialProof Security, where she helps people and companies keep their data safe by training and pentesting them on social engineering threats like Vishing and the many psychological tricks attackers employ to hack people – check it out...

October 11, 2022 /

[Cybersecurity Accountability Regulation? Your Opinion Matters…]

CISOs and CSOs are already on the hook and are the first ones to take the fall for breaches regardless of whether they fought for additional investments in people, processes, and technology. But what about accountability for the C-Suite and BOD?

October 6, 2022 / 1 minute read

[Container Escape: All You Need is Cap (Capabilities)]

Container Escape is considered the 'Holy Grail' of the container attack world - it allows an attacker to escape from a container to the underlying host, and by doing so the attacker can move laterally to other containers from the

host or perform actions on the host itself...

October 5, 2022 / 9 minute read

[Leveraging Indicators of Behavior for Early Detection]

The key to early detection of advanced operations such as the SolarWinds attacks is in leveraging Indicators of Behavior (IOBs) to level-up to a more efficient and effective Operation-Centric approach to detecting the whole of an attack as opposed to responding to individual, uncorrelated alerts...

October 5, 2022 / 4 minute read

[Blue Teaming on macOS with eslogger]

In this edition of the Blue Team Chronicles, we assess the capabilities of eslogger, a new built-in macOS tool, and show how defenders can use this tool to better understand malicious activities on macOS and build new detection approaches...

October 4, 2022 / 8 minute read

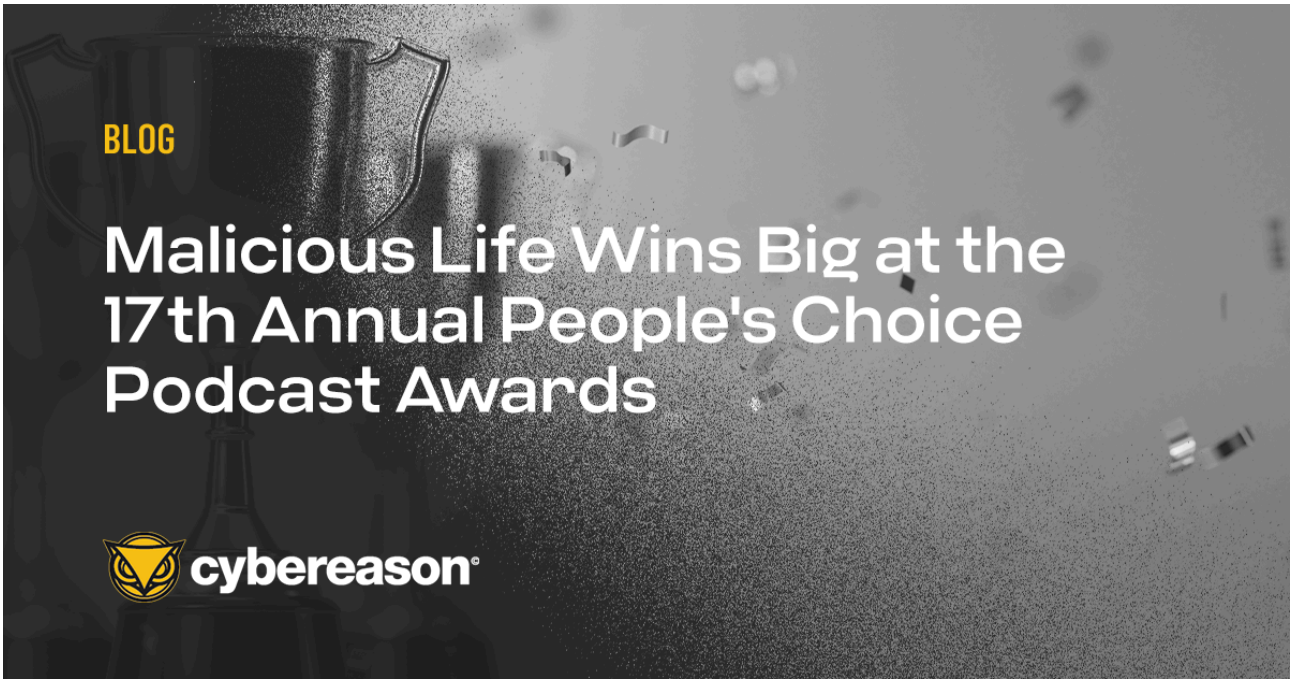
[Malicious Life Podcast: Hacking Stock Markets Part 1]

Some stock traders are willing to go to great lengths to get information before anyone else, even hacking into trading technologies to gain an unfair advantage and make a fortune along the way–check it out...

October 4, 2022 /


BLOG
THREAT ALERT: ProxyNotShell - Two Critical Vulnerabilities Affecting MS Exchange
cybereason


BLOG
A Guide to More Efficient and Effective SOC Teams
cybereason


BLOG
Malicious Life Wins Big at the 17th Annual People's Choice Podcast Awards
cybereason


BLOG
Webinar October 18th 2022: The True Cost of Ransomware - Evaluating Risk and How to Avoid Attacks
cybereason

[Cloud Authentication: A Guide to Choosing the Right Solution]

Authentication is one of the main elements of a cloud application, as it provides the ability to control access to your application. Need to pick an authentication solution and don't know where to start? This write-up will guide you in choosing an authentication solution that will suit your needs...

September 29, 2022 / 5 minute read

[Webinar October 13th 2022: Ten Considerations for More Efficient Security]

Join us on October 13th to hear from-the-field tips on how to create world-class efficiencies, including ways to find efficiencies within your tech stack, tips on how to recruit and manage a successful team, practical tips any

team can take to reduce event burden, how the Cybereason Defense Platform can create a 10x boost in efficiencies and more...

September 29, 2022 / 1 minute read

[Malicious Life Podcast: What It's Like to Fight LulzSec]

As their name implies, LulzSec was known for trolling their victims:, and while their childish behavior might have fooled some people into thinking that LulzSec was harmless, the story you're about to hear will show they were anything but – check it out...

September 28, 2022 /

[Defending Against Supply Chain and Ransomware Attacks]

Attacks on organizations that originate from third-party partners and service providers are expected to rise in the coming years as attackers look for weak links in software supply chains in an effort to “attack one to attack all..."

September 27, 2022 / 4 minute read

[Next Generation Antivirus Prevention Redefined]

Traditional antivirus tools from legacy vendors spot the easy stuff but struggle to prevent novel threats from causing damage. That is why Cybereason is announcing its latest prevention technologies to detect and block all threats from commodity malware to the never before seen...

September 22, 2022 / 1 minute read

[How XDR Reduces the Total Cost of Security Operations]

AI-driven XDR solution unifies telemetry analysis to optimize efficacy, improves operational efficiency at scale, and eliminates detection blind spots by generating deeply contextual correlations from endpoints, identity

management, workspaces, application suites, the cloud and more...

September 21, 2022 / 3 minute read

[Webinar October 26th 2022: NGAV Redefined]

In this webinar we will hear from Cybereason CTO and co-founder Yonatan Striem-Amit about how threats are changing; Tim Amey, Field CTO about how Cybereason prevention layers stop malware in its tracks; and Cody Queen, Product Marketing Manager share the latest prevention tools developed by Cybereason to stop the most novel attack techniques...

September 21, 2022 / 1 minute read

[Cyber Defenders Council: Is it Time for Cybersecurity Regulation?]

The report showcases best practices that Council members have used to align business executives around a common understanding of cyber risk and also explores a potentially controversial solution to the business-cybersecurity alignment gap: cybersecurity accountability regulation...

September 20, 2022 / 2 minute read

[Preparing Your Organization for a Ransomware Attack]

You cannot defend against RansomOps in traditional ways because it’s not a traditional threat, and a focus on detecting the ransomware executable alone is risky because that is the tail-end of a longer attack sequence, where the adversary already has unfettered access to your network...

September 20, 2022 / 4 minute read

[Malicious Life Podcast: King Kimble - Kim DotCom]

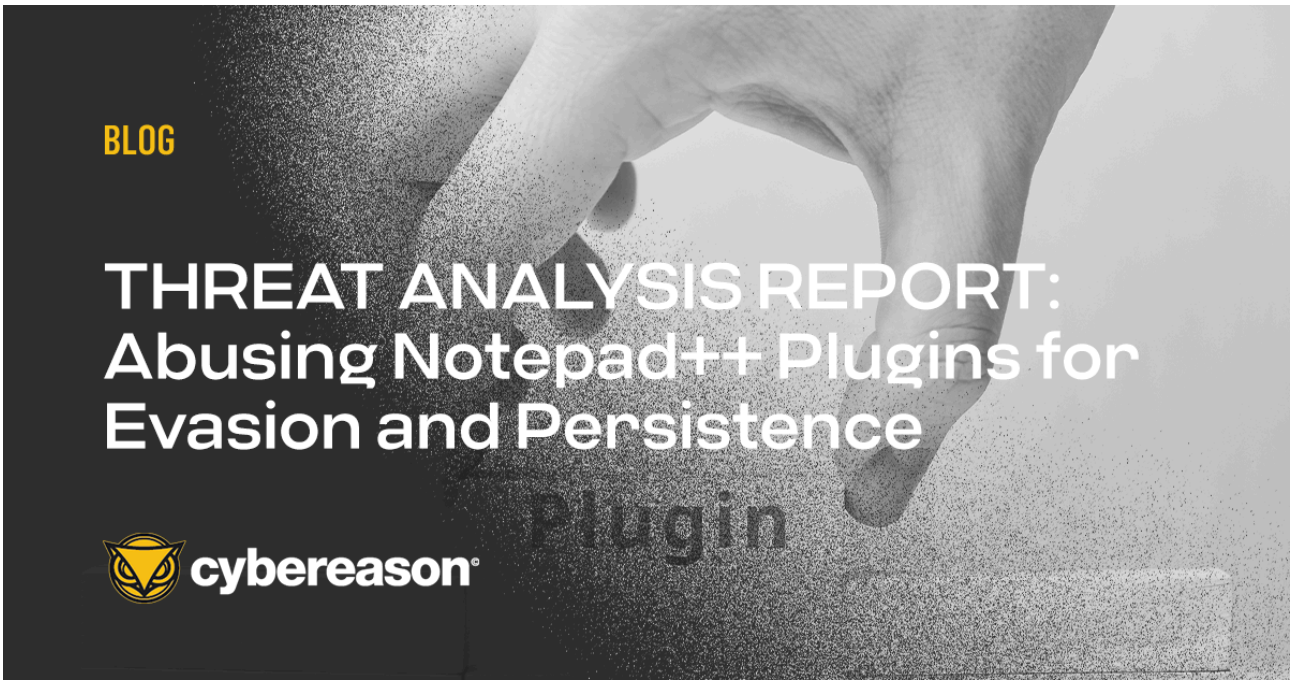
The US government says that Kim Schmitz, better known as Kim DotCom, is the leader of a file sharing crime ring. He sees himself as an internet freedom fighter: a fugitive on the run from vindictive overly-powerful governments. Can King Kimble escape the wrath of the USA? Check it out...

September 19, 2022 /

[Ransomware Head to Head: Don't Follow the CRWD]

When ransomware threatens to shut down your business, the most critical measures of success is the ability to detect malicious activity in real time...

September 15, 2022 / 4 minute read



Source: https://www.cybereason.com/blog/lockbit-ransomware-wants-to-hire-your-employees