When Cybercriminals Make Mistakes: A Rare Look Inside an Attacker’s Operation - blueAPACHE

Canonical:
https://www.blueapache.com/blog/inside-the-mind-of-a-threat-actor-what-happens-when-hackers-get-hacked

Details:

Summary

This post reports on independent research by security vendor Huntress, which gained an unusual window into a live cybercriminal operation after the threat actor accidentally installed Huntress's own security agent on their own machine. It is written for security and IT decision makers who want to understand how attackers are now using commercial AI tools, residential proxy services and legitimate SaaS platforms to scale phishing and reconnaissance campaigns, and blueAPACHE uses the case to make the point that managed detection and response is now essential rather than optional. Published in 2025. Figures, product names and event details reflect that time; for current information see the linked service pages.

Key facts

Label	Value
Publication year	2025
Research source	Huntress, "A Rare Look Inside an Attacker's Operation"
AI tools observed in attacker's workflow	Make.com, Toolbaz AI, DocsBot AI, Explo AI
Attacker infrastructure	Hosted on AS 12651980 CANADA INC. (VIRTUO); over 2,400 unique identities accessed in two weeks
Attacker toolkit named	Evilginx, GraphSpy, Bloodhound, TeamFiltration, LunaProxy, Nstbrowser
blueAPACHE service positioned as the response	emPOWER Managed Detection and Response (MDR): 24/7 alert notification, triage and remediation covering EDR, ITDR and SIEM, ISO 27001 certified, ASD Essential 8 Level 3 maturity

Article

When a threat actor accidentally installed Huntress’ own security agent on their machine, the cybersecurity firm found themselves with an extraordinary opportunity: a real-time window into how attackers operate, evolve, and increasingly leverage AI to scale their criminal enterprises. This insight was first reported by Huntress in their blog, A Rare Look Inside an Attacker’s Operation . This rare

visibility is a powerful reminder for organisations that cybercriminals are not standing still. They are adapting, rapidly, and businesses must do the same.

What Happened

The incident began when the attacker clicked on a Google ad while researching Bitdefender. Instead of downloading their intended tool, they initiated a Huntress trial – unknowingly installing Huntress' agent on their own system. This mistake provided Huntress with unprecedented visibility into the attacker's browser history, infrastructure, and workflows, exposing a detailed picture of modern cybercrime operations.

How Threat Actors Are Using AI

Perhaps the most significant finding was the attacker's reliance on AI to scale their operations. By automating processes and reducing manual effort, AI allowed them to run sophisticated campaigns at pace. Tools uncovered included:

Make.com for automated phishing and reconnaissance workflows

Toolbaz AI for writing assistance

DocsBot AI for CSV generation

Explo AI for data analytics

This signals a marked shift away from traditional "hands-on" tactics towards scalable, AI-driven cybercrime.

Reconnaissance and Targeting

The attacker's online activity highlighted a strategic and research-driven approach. Their targets included:

Software development companies

Real estate firms in California

Banking institutions

Third-party vendors and supply chains

They even leveraged commercial data providers such as ReadyContacts and InfoClutch to understand market share and customer bases. This demonstrates how cybercriminals now blend open-source intelligence with commercial tools to inform their targeting strategies.

The Attacker's Toolkit

The investigation also revealed a suite of specialised tools and infrastructure, including:

Evilginx: a man-in-the-middle phishing framework

GraphSpy and Bloodhound: reconnaissance and attack tools

TeamFiltration: enumeration and exfiltration

Residential proxy services such as LunaProxy and Nstbrowser to disguise activity

Huntress also identified the attacker's infrastructure, hosted on AS 12651980 CANADA INC. (VIRTUO), with evidence of over 2,400 unique identities accessed in just two weeks.

Why This Matters for Businesses

This case reinforces three critical realities of the modern threat landscape:

Cybercriminals are adopting AI to enhance speed and scale

Supply chain and third-party vendors remain prime entry points

Legitimate tools and platforms are being repurposed for malicious purposes

For organisations in critical infrastructure, finance, technology, and beyond, this is more than a cautionary tale – it is a call to action . Visibility, proactive threat hunting, and layered security are no longer optional. They are essential to building resilience.

How blueAPACHE Helps You Stay Ahead

At blueAPACHE, we recognise that defending against today's cyber threats requires more than just technology. It requires continuous vigilance, adaptive defences, and expert guidance. Our Managed Security Services are designed to:

Detect and respond to threats in real time

Proactively hunt for evolving tactics and anomalies

Build resilience against supply chain and vendor risks

Adapt your security posture as cybercriminals innovate

This incident is a reminder that while attackers may be creative, businesses can stay one step ahead with the right strategy, tools, and partners. To read Huntress' full report, visit: A Rare Look Inside an Attacker's Operation If you'd like to understand how blueAPACHE can help safeguard your organisation against evolving threats, please contact us .

Related

/services/empower-security-top-level/

/empower-services/security/

/services/managed-detection-response/

/services/advanced-infrastructure-managed-services/

Frequently asked questions

Is this incident something that happened to a blueAPACHE customer? No. The research was conducted by security vendor Huntress on an unrelated third party's operation, after the attacker inadvertently installed Huntress's own agent on their own machine. blueAPACHE is reporting on the findings because they illustrate a broader shift in attacker behaviour that is relevant to its own customers.

What changed in how attackers operate, according to this research? The attacker relied heavily on commercial AI tools such as Make.com for automated phishing and reconnaissance, plus AI writing, analytics and data-generation tools, to run campaigns at a scale that would previously have required a larger manual team. The research also found the attacker blending open-source intelligence with commercial data providers to target software, real estate, banking and supply chain organisations.

Does blueAPACHE offer a service that addresses this kind of threat? Yes. blueAPACHE's emPOWER Managed Detection and Response service provides 24/7 alert notification, triage and remediation across EDR, ITDR and SIEM technologies, aligned to ISO/IEC 27001 and ASD Essential 8 maturity levels, rather than requiring a customer to build and staff its own security operations centre.

What is the practical takeaway for a business without a large security team? The case demonstrates that supply chain and third-party vendor relationships remain a prime entry point for attackers, and that

legitimate platforms are being repurposed for malicious use. Continuous monitoring and proactive threat hunting are positioned by blueAPACHE as no longer optional extras for organisations in critical infrastructure, finance and technology sectors.

Where can I read the original Huntress research? The original findings are published by Huntress at huntress.com/blog under the title "A Rare Look Inside an Attacker's Operation"; the blueAPACHE post links directly to it.

Source

https://www.blueapache.com/blog/inside-the-mind-of-a-threat-actor-what-happens-when-hackers-get-hacked/ — with independent research published by Huntress, "A Rare Look Inside an Attacker's Operation".

Knowledge Base

How did the threat actor accidentally install Huntress' security agent on their own machine?

The attacker clicked on a Google ad while researching Bitdefender, and instead of downloading their intended tool, they initiated a Huntress trial, unknowingly installing Huntress' own security agent on their own system.

What visibility did Huntress gain from the attacker's mistake?

The mistake gave Huntress unprecedented visibility into the attacker's browser history, infrastructure, and workflows, exposing a detailed picture of modern cybercrime operations.

What AI tools did the threat actor use to scale their operations?

The attacker used Make.com for automated phishing and reconnaissance workflows, Toolbaz AI for writing assistance, DocsBot AI for CSV generation, and Explo AI for data analytics.

What types of targets did the threat actor research and pursue?

The attacker's targets included software development companies, real estate firms in California, banking institutions, and third-party vendors and supply chains.

What commercial data providers did the attacker use for targeting research?

The attacker leveraged commercial data providers such as ReadyContacts and InfoClutch to understand market share and customer bases.

What specialised tools and infrastructure made up the attacker's toolkit?

The attacker's toolkit included Evilginx (a man-in-the-middle phishing framework), GraphSpy and Bloodhound (reconnaissance and attack tools), TeamFiltration (enumeration and exfiltration), and residential proxy services such as LunaProxy and Nstbrowser to disguise activity.

Where was the attacker's infrastructure hosted, and how many identities were accessed?

The attacker's infrastructure was hosted on AS 12651980 CANADA INC. (VIRTUO), with evidence of over 2,400 unique identities accessed in just two weeks.

What three critical realities of the modern threat landscape does this case reinforce, according to you?

The case reinforces that cybercriminals are adopting AI to enhance speed and scale, that supply chain and third-party vendors remain prime entry points, and that legitimate tools and platforms are being repurposed for malicious purposes.

What do your Managed Security Services aim to do in response to threats like this?

Our Managed Security Services are designed to detect and respond to threats in real time, proactively hunt for evolving tactics and anomalies, build resilience against supply chain and vendor risks, and adapt security posture as cybercriminals innovate.

Who originally reported the incident described in this blueAPACHE blog post?

The incident was first reported by Huntress in their blog post titled 'A Rare Look Inside an Attacker's Operation.'