Talent Need Not Apply

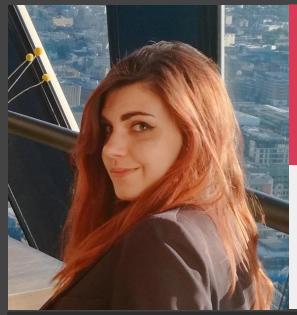
Tradecraft and Objectives of Job-themed APT Social Engineering

PwC Global Threat Intelligence

Prepared for Black Hat USA

August 2022

Introductions



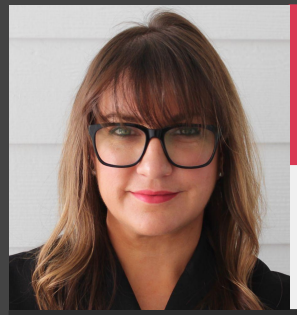
Sveva Vittoria Scenarelli

Principal Analyst
PwC UK

Working at PwC for nearly 4 years, APAC-based APT focus

- Loves tracking campaign evolutions over time
- Regularly unmasking North Korea-based threat actors' activities (VirusBulletin 2021, CONFidence 2021 and 2020)

@cyberoverdrive



Allison Wikoff

Director
PwC US

Global Threat Intelligence Lead for PwC Americas

- 20 years in cyber, IR, network defense, threat intelligence
- 7+ years research focus on Iran
- Lives for threat actor mistakes

@SaltyWikoff

The Great Resignation is showing no signs of slowing down

"The Great Resignation" is not slowing down

APTs are increasingly using job-themed lures

Unveil threat actors' initial access TTPs and motives

Explain how to recognise social engineering attempts

PwC 2022 Global Workforce Hopes and Fears Survey https://www.pwc.com/workforcehopesandfears

Black Artemis

A prolific recruiter: Black Artemis

Aliases	HIDDEN COBRA, Lazarus Group
Related threat actors	Black Artemis / temp.Hermit Andariel Bluenoroff
Active since	2007
Motivation	Sabotage Espionage Cyber crime
Targets	Aerospace, DIB, Manufacturing…

Dream job, delivered

Social media

Recruiter personas

Email phishing

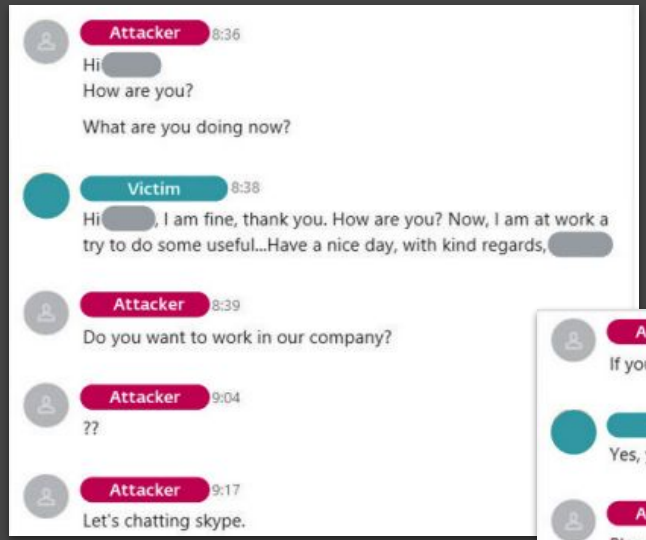
Malicious attachments

Messaging apps

“Recruiter” follow-up

Domain spoofing

lm-careers[.]com
global-job[.]org
indeedus[.]org



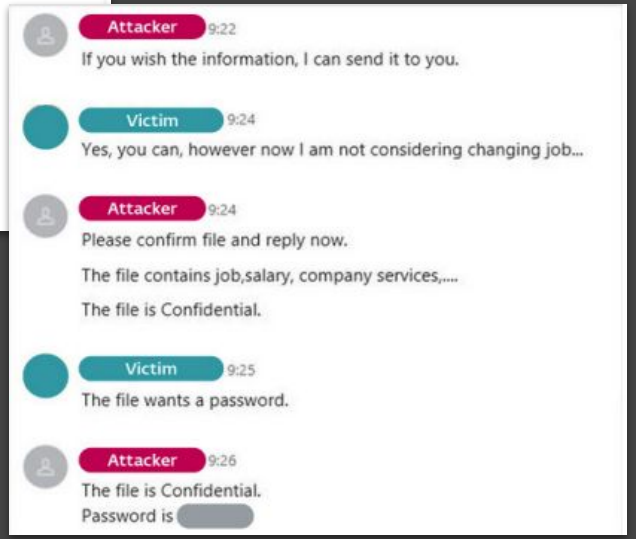


Image source:
https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_Operation_Interception.pdf

Domain spoofing

Web exploitation

CVE-2022-0609
RCE in Chrome

User awareness

Before clicking links, look up the original site.

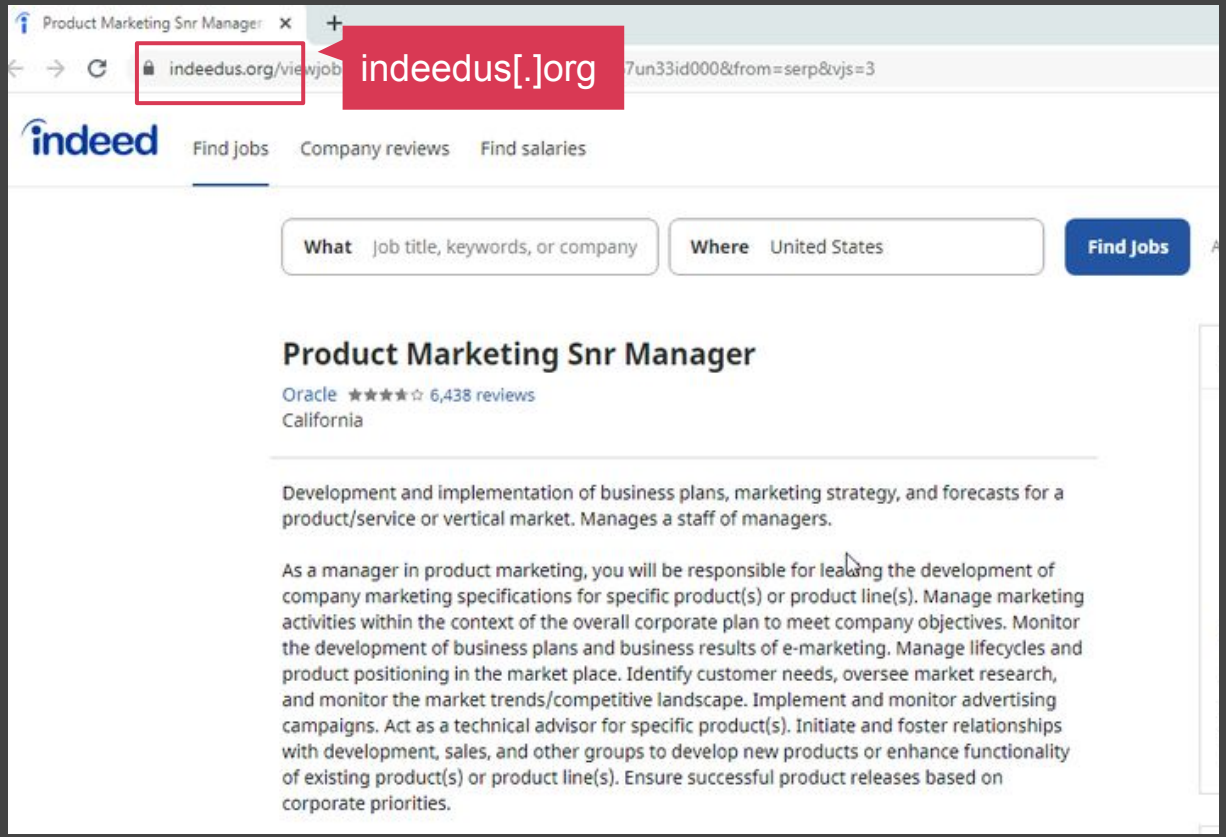
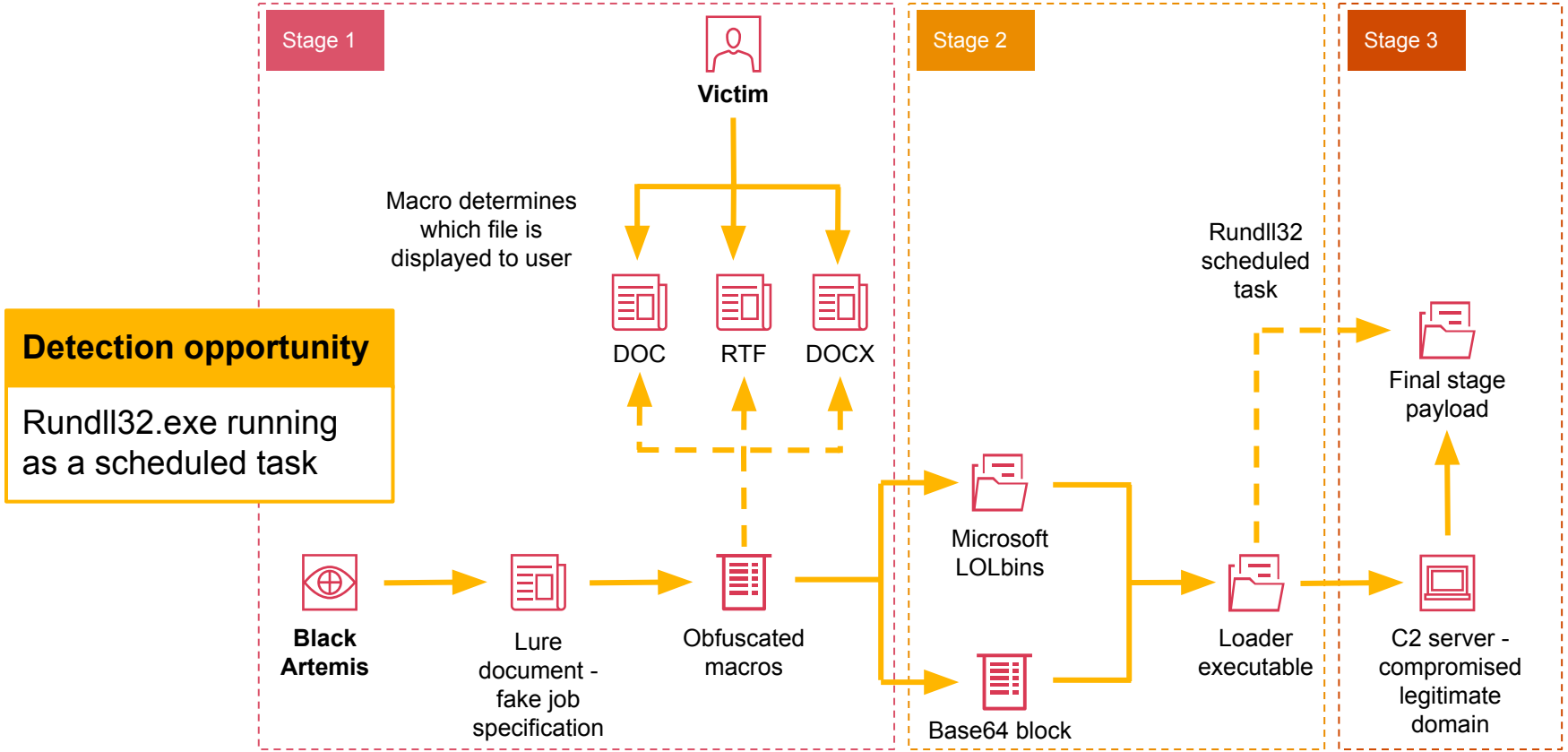
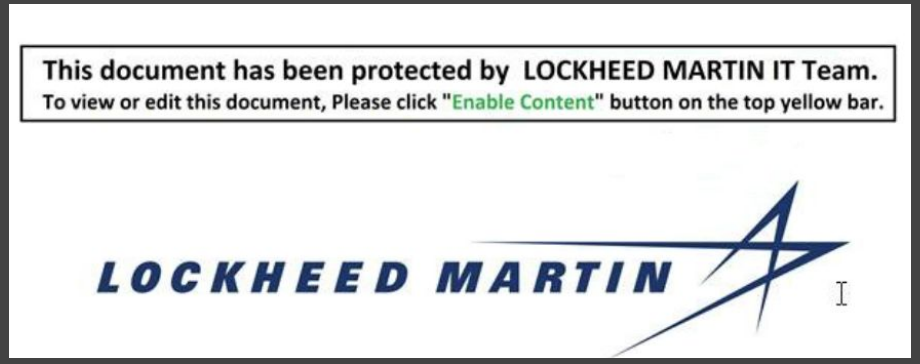


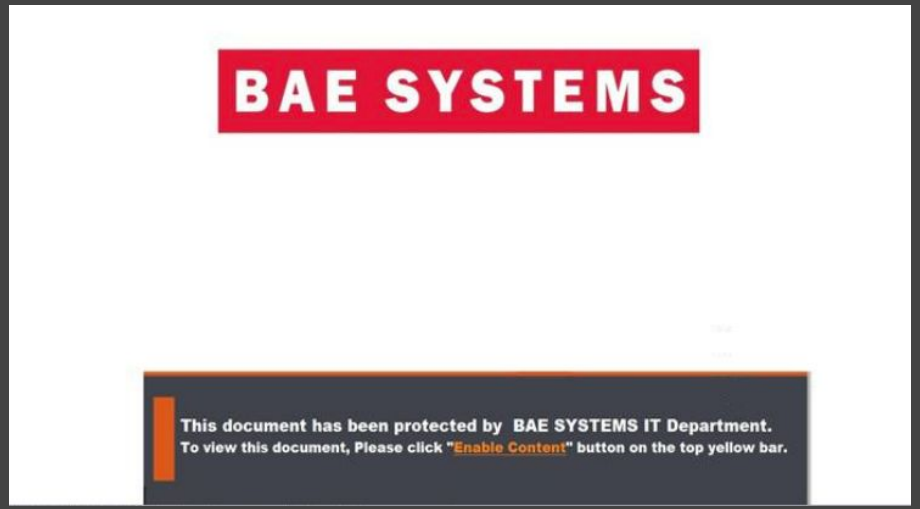
Image source: https://blog.google/threat-analysis-group/countering-threats-north-korea/

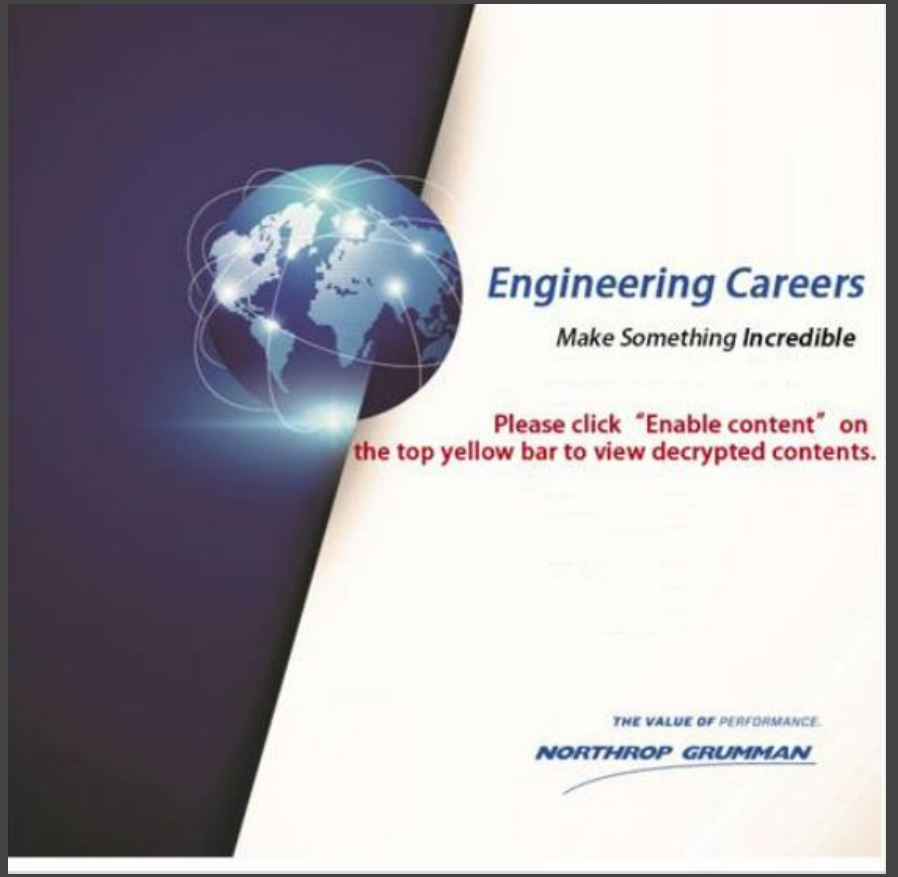
Black Artemis example intrusion chain



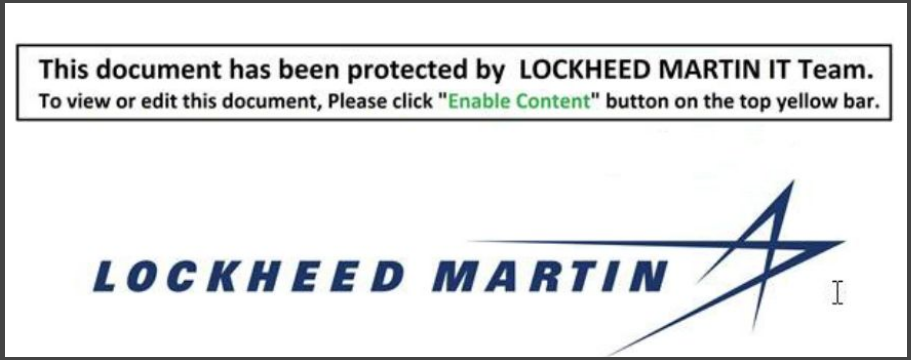
A prolific recruiter: Black Artemis

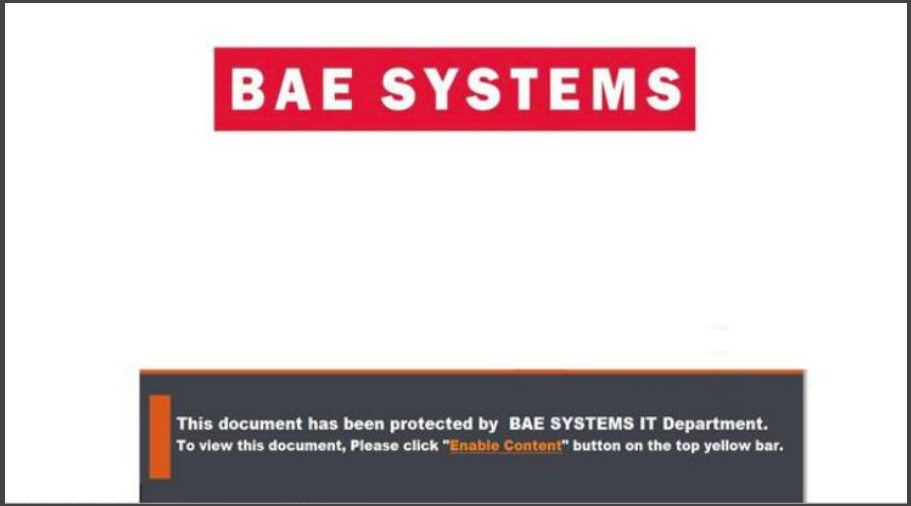






Anatomy of a Black Artemis job-themed lure





Author	Mickey
File name	“Opportunity”, “Salary”
Theme	Aerospace, Defence
Macros	Converting UUIDs into 32-bit or 64-bit shellcode payloads
Function definitions	Aliasing WinAPIs to be used, like `CreateHeap`, `HeapAlloc`
Message boxes	`/MsgBox \"Cannot open the document.\", [A-Za-z]{5,9} \+ vbInformation/`
Heuristics	Excessive variable definitions

Black Alicanto

North Korea and cryptocurrency


CRYPTOTHEFT —

North Korea suspected in latest bitcoin heist, bankrupting Youbit exchange

Breach bankrupts Seoul-based company after it reformed in wake of a previous heist.

SEAN GALLAGHER - 12/20/2017, 8:52 PM

Illegal financing is an existential imperative


U.N. experts point finger at North Korea for $281 mln cyber theft, KuCoin likely victim

By Michelle Nichols and Raphael Satter


FOR IMMEDIATE RELEASE

Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe

Indictment Expands 2018 Case that Detailed Attack on Sony Pictures and Creation of WannaCry Ransomware by Adding Two New Defendants and Recent Global Schemes to Steal Money and Cryptocurrency from Banks and


US blames North Korean hacker group for $625 million Axie Infinity theft

The US Department of Treasury says Lazarus is behind the attack

A crypto recruiter: Black Alicanto

Aliases	DangerousPassword, CryptoCore, CryptoMimic
Related threat actors	Bluenoroff
Active since	2018
Motivation	Cyber crime
Targets	Financial Services

(Ad)venture capital

Direct email

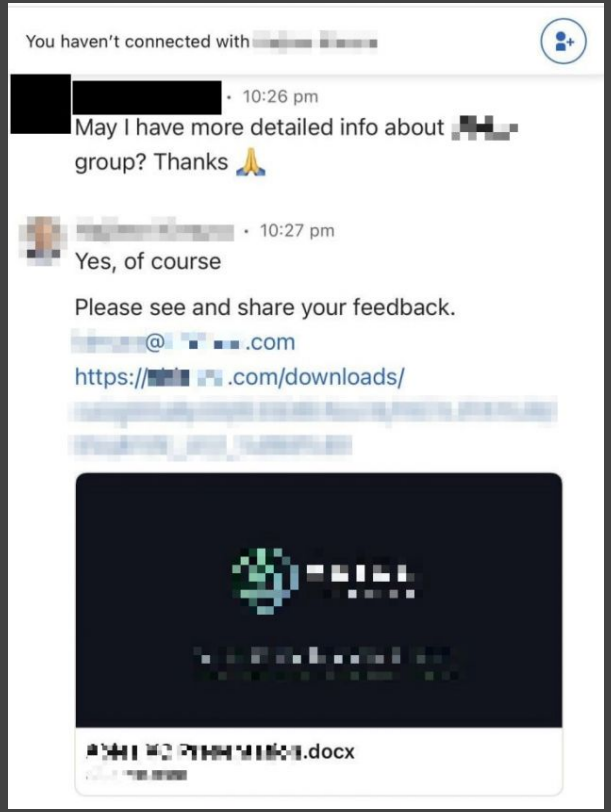
ZIP/RARs with LNK files

Fwd email

Fake VC pitches

Social media

“Recruiter” personas



Domain spoofing

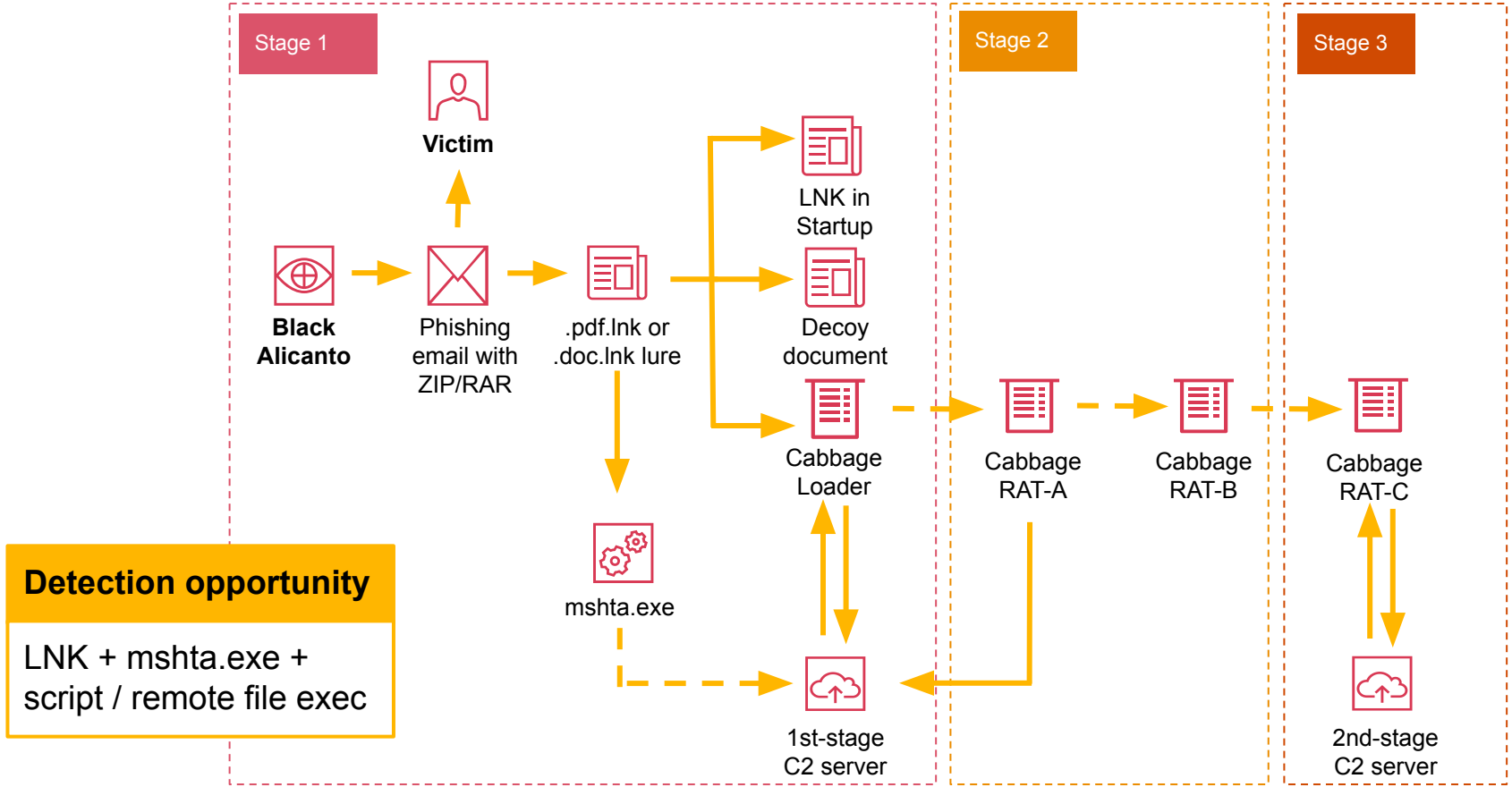
www[.]gsachshr[.]com
ny[.]silvergatehr[.]com
mail[.]daiwa-inv[.]com

Hunting opportunity

Porkbun Registrar + specific Apache, PHP, OpenSSL versions in server HTTP response

Image source: https://securelist.com/the-bluenoroff-cryptocurrency-hunt-is-still-on/105488/

Black Alicanto example intrusion chain



Anatomy of a Black Alicanto job-themed lure

Black Alicanto, September 2021

File type	.pdf.lnk, .docx.lnk
File name	“Opportunities”, “Salary”
Theme	Finance, Blockchain
Machine ID	`desktop-j54m766`, `desktop-70c1dv0`, others
LNK execution	`/c start /b %SystemRoot%\System32\mshta` [Target URL]
Heuristics	Double extension files, LNK file invoking a command, LNK file invoking MSHTA
C2 elements	Spoofing Google, cloud services

Job hopping in North Korea

Blockchain Intelligence Group

Welcome

When you work for Commerz Real AG, by engineering the future wellbeing of humanity, you'll be taking important steps for your own future. Whatever your role, you can have the satisfaction of bringing your best thinking to the toughest challenges confronting humanity.

Black Alicanto, September 2021

Has an operator moved teams?

LOCKHEED MARTIN

Welcome

When you work for Lockheed Martin, by engineering the future wellbeing of humanity, you'll be taking important steps for your own future. Whatever your role, you can have the satisfaction of bringing your best thinking to the toughest challenges confronting humanity.

Black Artemis, March 2021

North Korea and the job market: IT and APT

DPRK IT workers seeking IT jobs abroad

Roles range from app/web dev to digital coins

Operate through proxy IDs

Cases of access handoff to APT operators

Causes and consequences

Funding regime & nuclear weapons program

Companies risk breaching sanctions

The job market is a key area of North Korean revenue generation - whether through APT activity or IT workers.

Recruiters in the East

Iran-based Threat Actors Who Love a Recruitment Theme

Yellow Garuda

Charming Kitten / PHOSPHORUS / ITG18 / UNC788

Yellow Liderc

TortoiseShell / TA456 / Imperial Kitten

Yellow Maero

APT34 / COBALT GYPSY / OilRig

Yellow Dev 13

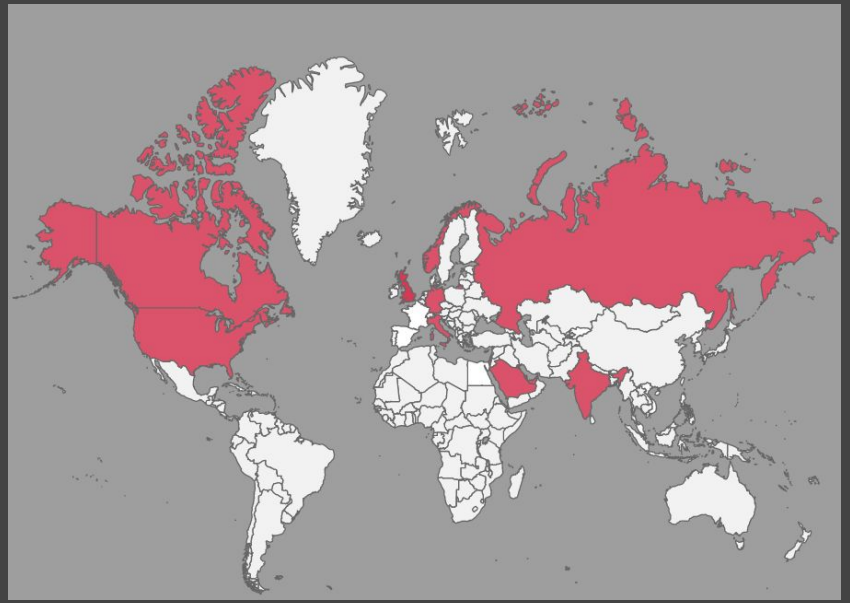
BOHRIUM / TA455 / Imperial Kitten

(This is not an exhaustive list)

Yellow Dev 13

Who is Yellow Dev 13?

Aliases	TA455, BOHRIUM
Related threat actors	Imperial Kitten
Active since	2019
Motivation	Espionage
Targets	Energy, Technology, Maritime, Telecommunications, Semiconductor, Logistics



Yellow Dev 13 Geographical Targeting Source: PwC Threat Intelligence

Fake Stuff Everywhere

Spoofed Companies

Oil and gas
Energy
Engineering
Recruiting (general/specific)

Fake Companies

Recruiting (general)

Fake People

Recruiters
Trainers
AI generated profile pictures

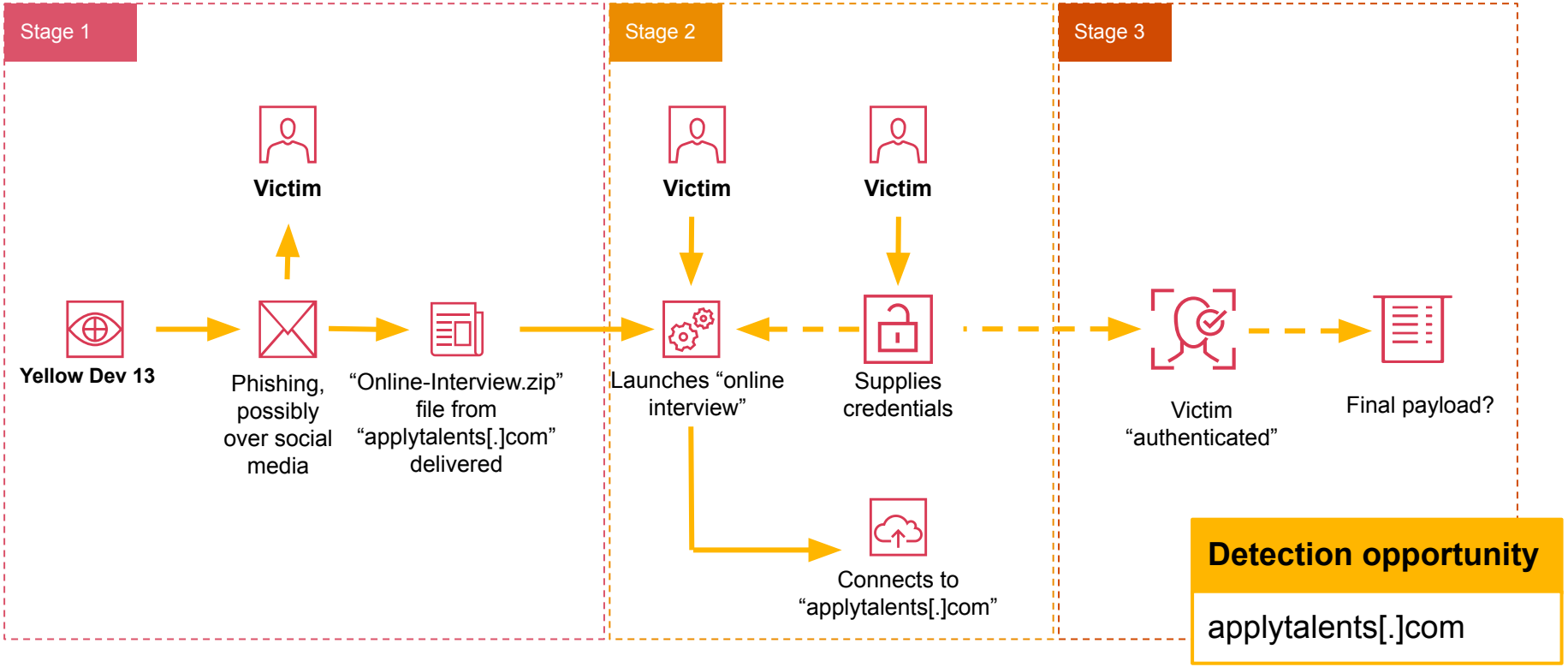
Associated Domains

applytalents[.]com
careers-finder[.]com

Hunting opportunity

Google searches find similar (bad) pages + Similar websites/names

“Apply Talents” Suspected Intrusion Chain

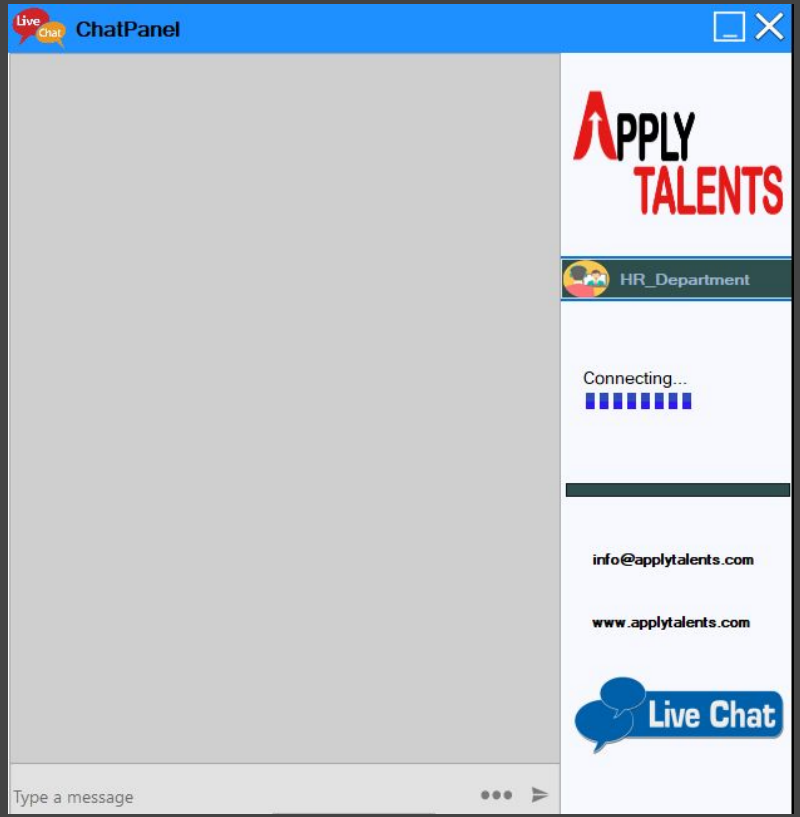


Apply Talents “online interview”

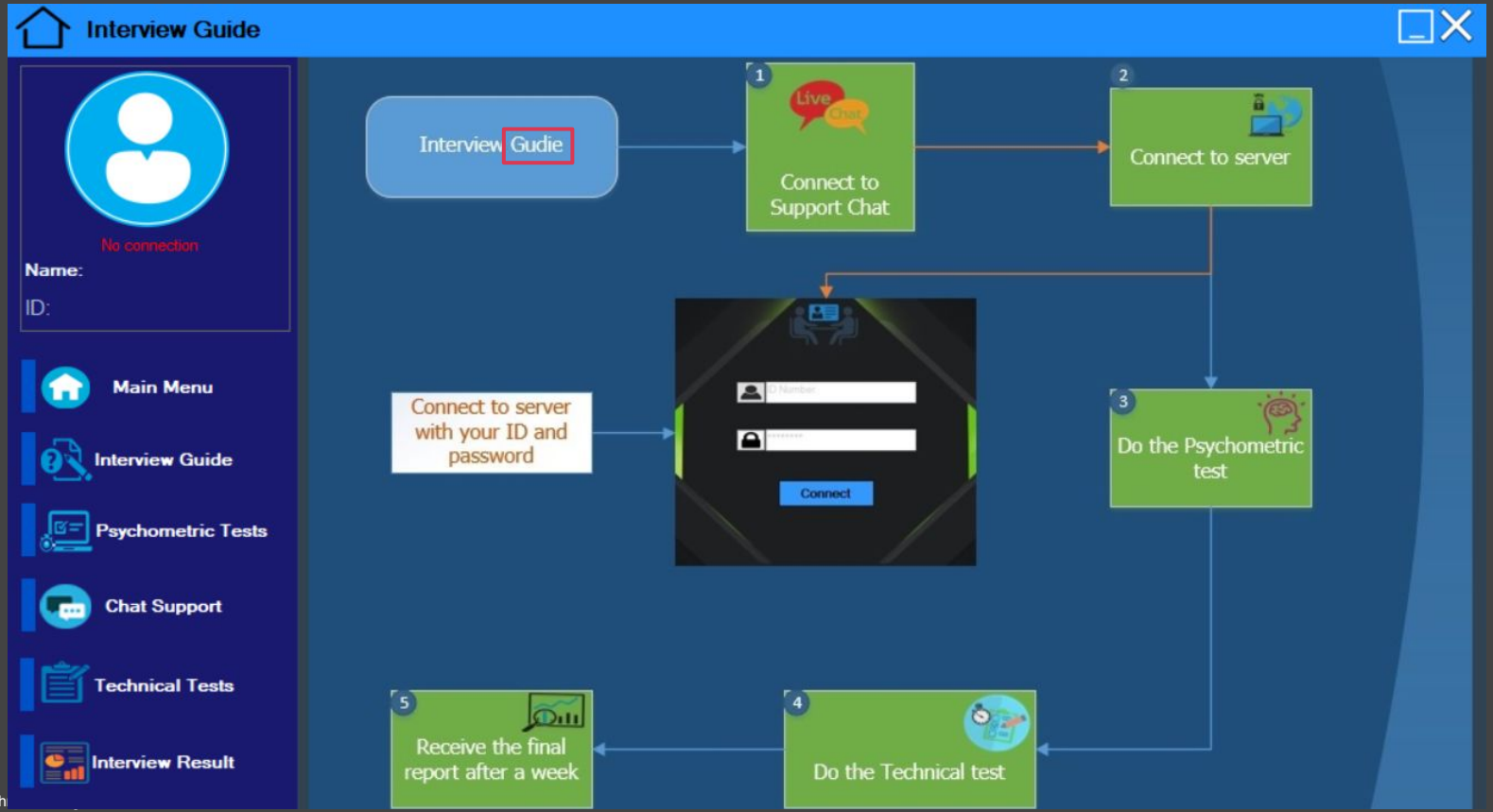
SHA256

851546167d6557a00ecbf7
ada0448f96b0c721c74bf69
54556ec319cda054584

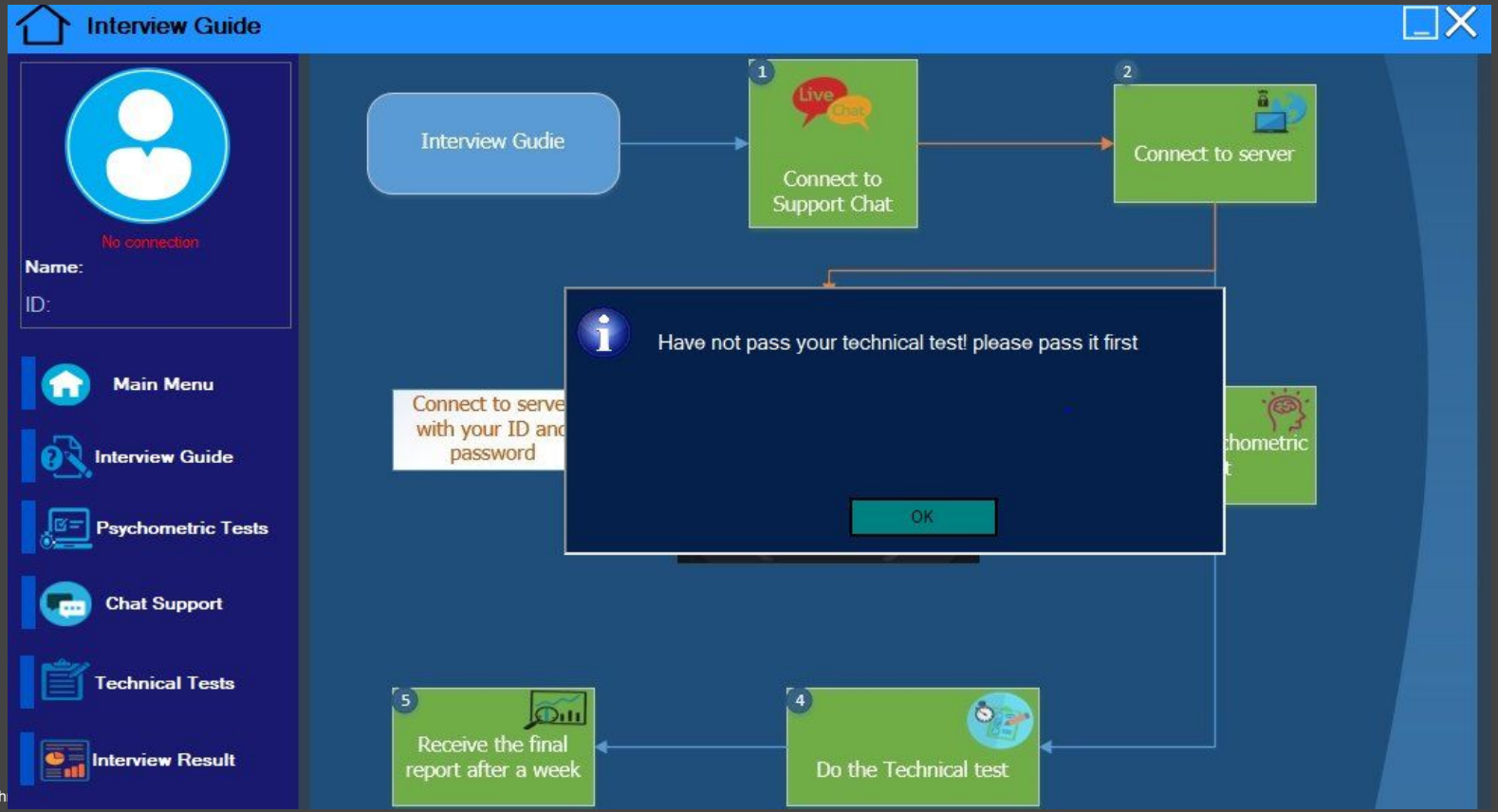
Apply Talents “online interview”



Apply Talents “online interview”



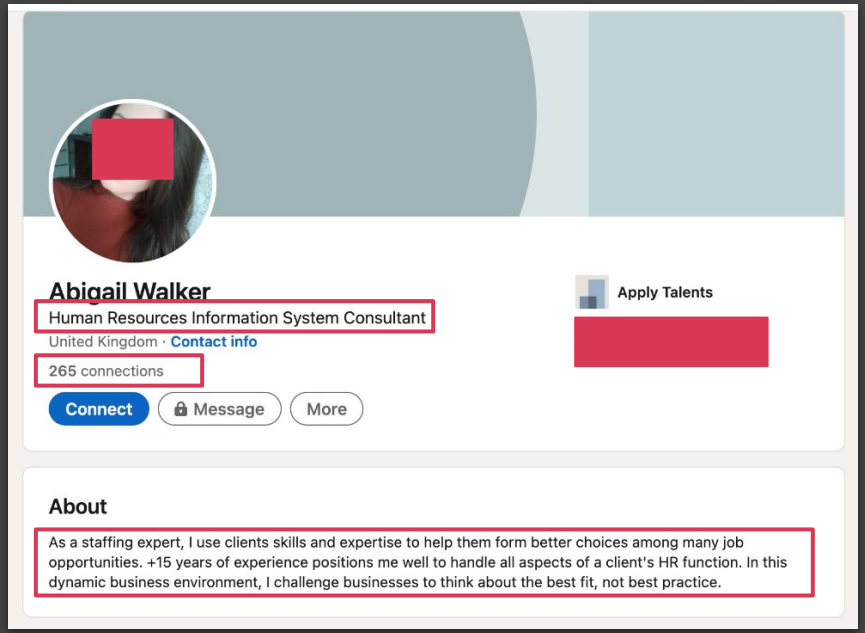
Apply Talents “online interview”

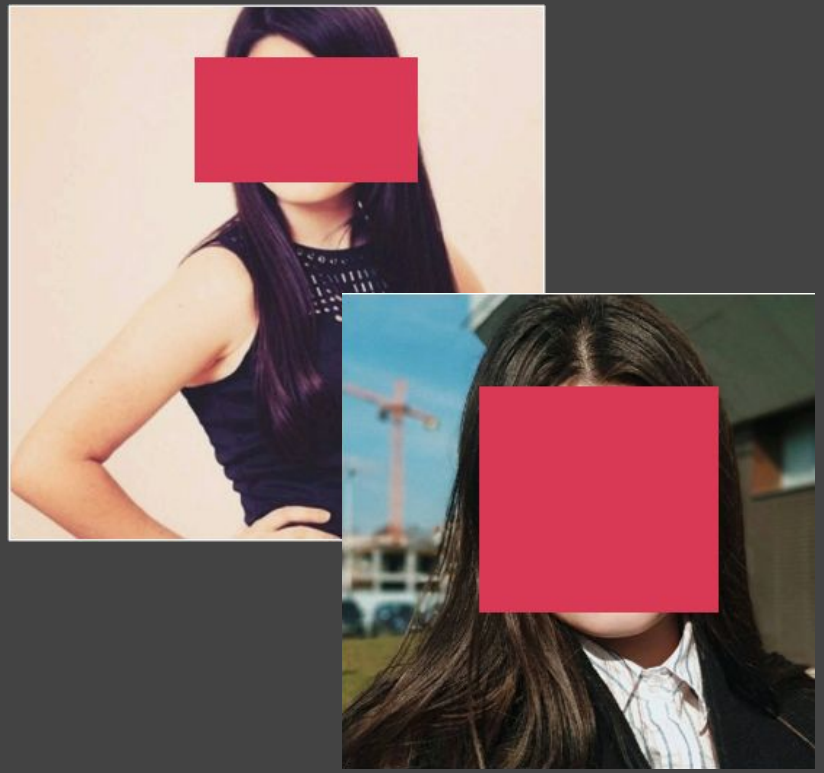


“We’ll help you find a job that fulfil your desires”

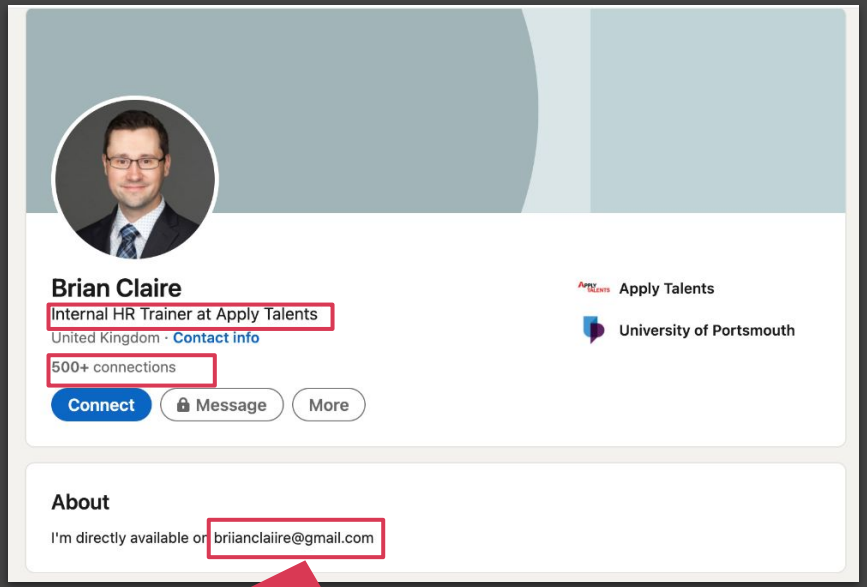
- Careers-finder[.]com

“Apply Talents” on LinkedIn



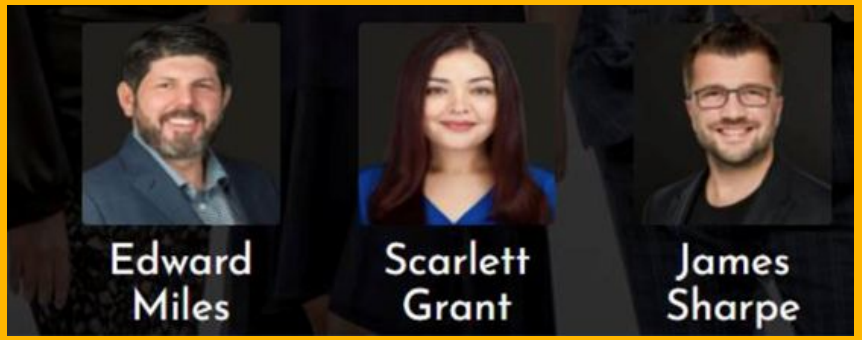


“Apply Talents” on LinkedIn

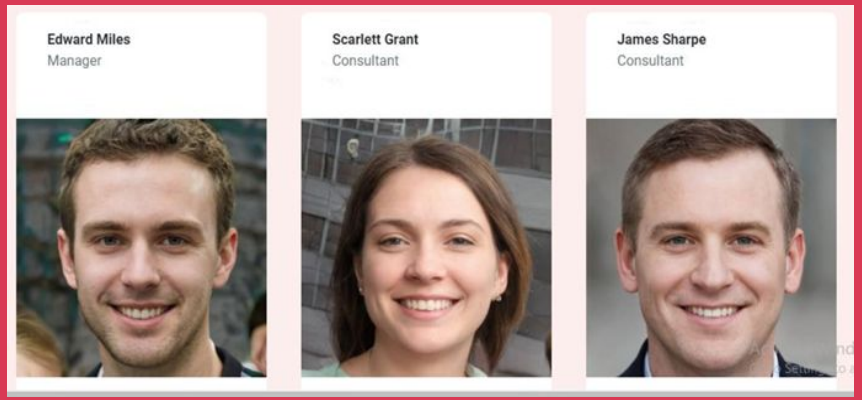


briianclaiire[@]gmail.com

Meet the team



“Apply Talents”



“Careers Finder”

“Edward Miles”

Apply Talents

Careers Finder

“Scarlett Grant”

Apply Talents

Careers Finder

“James Sharpe”

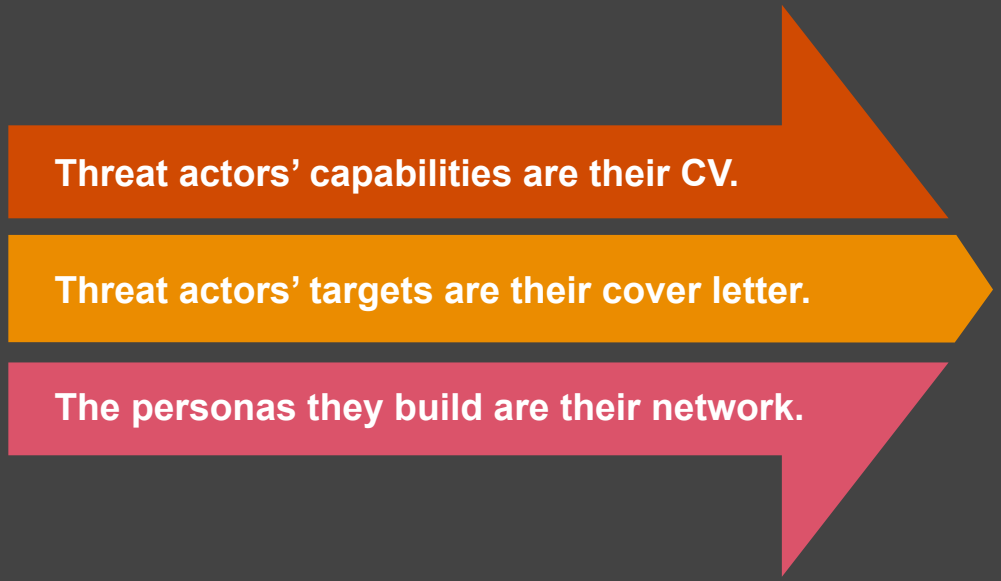
Apply Talents

Careers Finder

Other Fake People

Final Round
(Key Takeaways)

What's your dream job?

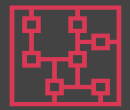


Understanding a threat actor is a bit like an interview - but you want to learn how to stop them, not hire them.

Key Takeaways

Threat actors are capitalizing on the great resignation

Social engineering still works, continues to evolve



Employees personal computing habits impact organizational security

Thank you!

pwc.com
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence.html

References

References

PwC Github Repo
https://github.com/PwCUK-CTO/BlackHat-USA-2022-Talent-Need-Not-Apply

PwC 2022 Global Workforce Hopes and Fears Survey
https://www.pwc.com/workforcehopesandfears

DPRK-based threat actor references

Black Artemis
'Operation In(ter)ception', ESET
https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_Operation_Interception.pdf
'Operation Dream Job', ClearSky Cyber Security
https://www.clearskysec.com/wp-content/uploads/2020/08/Dream-Job-Campaign.pdf
'Countering Threats from North Korea', Google
https://blog.google/threat-analysis-group/countering-threats-north-korea/

Black Alicanto
'North Korea suspected in latest bitcoin heist, bankrupting Youbit exchange', Ars Technica
https://arstechnica.com/tech-policy/2017/12/north-korea-suspected-in-latest-bitcoin-heist-bankrupting-youbit-exchange/
'U.N. experts point finger at North Korea for $281 million cyber theft, KuCoin likely victim', Reuters
https://www.reuters.com/article/us-northkorea-sanctions-cyber-idUSKBN2AA00Q
'Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe', US DOJ
https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and
'US blames North Korean hacker group for $625 million Axie Infinity theft', The Verge
https://www.theverge.com/2022/4/14/23025739/north-korean-hacker-lazarus-axie-infinity-cryptocurrency-hack-theft-us-blames

References

‘Unveiling the CryptoMimic’, Hajime Takai, Shogo Hayashi & Rintaro Koike
https://vb2020.vblocalhost.com/uploads/VB2020-Takai-etal.pdf
‘Lazarus Group campaign targeting the cryptocurrency vertical’, WithSecure (formerly F-Secure)
https://labs.withsecure.com/assets/BlogFiles/f-secureLABS-tlp-white-lazarus-threat-intel-report2.pdf
‘The BlueNoroff cryptocurrency hunt is still on’, Kaspersky
https://securelist.com/the-bluenoroff-cryptocurrency-hunt-is-still-on/105488/
‘here's a dump of examples of the sneaky malicious phishing emails and messages and sites designed to trick you.’, Taylor Monahan,
https://twitter.com/tayvano_/status/1516225457640787969
Fact Sheet: Guidance on the Democratic People’s Republic of Korea Information Technology Workers’, US Department of the Treasury
https://home.treasury.gov/system/files/126/20220516_dprk_it_worker_fact_sheet.pdf
‘Here's how North Korean operatives are trying to infiltrate US crypto firms’, CNN
https://edition.cnn.com/2022/07/10/politics/north-korean-hackers-crypto-currency-firms-infiltrate/index.html
‘North Korea: Missile programme funded through stolen crypto, UN report says’
https://www.bbc.co.uk/news/world-asia-60281129

Iran-based

‘Q1 2022 Meta Quarterly Adversarial Threat Report’, Meta
https://about.fb.com/wp-content/uploads/2022/04/Meta-Quarterly-Adversarial-Threat-Report_Q1-2022.pdf
BOHRIUM Domain Seizure, Microsoft
https://news.microsoft.com/wp-content/uploads/prod/sites/358/2022/06/Doc.-No.-16-Ex-parte-TRO-SEALED.pdf