PRIVILEGED & CONFIDENTIAL

BLACKWIRED

London Market Forums

THE CYBER ARMS RACE

FIFTH THEATRE OF WAR IN UKRAINE

Enterprise Cyber Security is in a Cyber-Arms-Race. Runaway growth in cyberattacks means our adversaries have achieved escape velocity from our established security controls systems, including our people. Post-mortem reports are too late to stop Patient Zero Cyber Attacks – this is ‘Right-of-Bang’.

Being perfect in Patching, Software Currency, and all the other hyper-interdependencies of a mosaic defence requires concentration on everything. This dependency on the “whack-a-mole” security operations approach only works if you see all the moles.

Enterprise does not have a way to measure the effectiveness of Cyber Security spending in the active prevention of a Cyberattack. This is unsustainable.

Blackwired has established a new category in cyber security with an intelligence-led, proactive, cyber-attack prevention model based on the USMC’s, Combat Hunter programme ‘Left of Bang.’ The Zero Day Live (ZDL) platform takes a different approach to traditional "Detect & Respond" solutions.

THE CYBER ARMS RACE

FIFTH THEATRE OF WAR IN UKRAINE

The war in Ukraine has exacerbated and accelerated the Cyber Arms Race. 46 Zero Day Weapons attributable to the Ukraine conflict were observed created between November 2021 and July 2022.

The Cyber war begins long before the land war in late Feb 2022. On 17th December 2021 (for example) the Lockbit Group removed restrictions from ransomware code allowing 0Day Lockbit 2.0 to be used against the former CIS States. As a result, 45 million Ukrainian Citizen's Identities were stolen using Lockbit 2.0 and are now in Russian hands.

These campaigns have continued with false flag operations - Asylum Ambuscade - to disrupt and confuse communications amongst allies to specific targeting of Ukrainian infrastructure such as - Saints of Steal - which hit Power Generation Facility using JavaScript.

Post covid there was already a stockpile of cyber weaponry ready to be launched on enterprise but what is now being seen is an increase in modification and development of weapons. Blackwired anticipates a tidal wave of attacks on global targets when the conflict in Ukraine allows the resources of the bad actors to be focused elsewhere.

WEAPONS DEVELOPMENT IN 2022

BLACKWIRED ZERO DAY LIVE EXAMPLES

TWO SIGNIFICANT WEAPONS DEVELOPMENTS THAT CHANGE CYBER SECURITY FOREVER

19th APRIL 2022 - SILENT COMPROMISE 'CLICK-LESS' PHISHING ON ANDROID AND IOS.

- **0Day Pegasus Spyware**
- **UK Government and Spanish Government (PMs and Ministers) compromised**
- **UK PM Boris Johnson's personal phone compromised.**
- **NSO GROUP (Israel)**
- **Cost USD 25,000 per Target (complete persistent silent surveillance).**

15th JULY 2022 - GOOGLE SEO SEARCH POISONING - FILELESS WEAPON PAYLOAD DELIVERY (EXECUTES IN RAM) – USE OF 700 HIGH-TRAFFIC WEBSITES FOR DELIVERY.

- **0Day Gootloader – Loader (Remote Access Trojan)**
- **Targeting globally sensitive financial, military, automobile, pharmaceutical and energy sectors**
- **Uses sophisticated poisoning of Google Search Engine Optimisation to lure victims to fake websites**
- **700 different High-Traffic Compromised Websites are the weapons delivery network**

BLACKWIRED FIRST TO SEE – as at 19 Jul 22 - ONLY BLACKWIRED PREVENTS/IMMUNISES THESE WEAPONS

BLACKWIRED

CYBER TRACKING – CYBER RISK MODELING / UNDERWRITING SUPPORT

Blackwired is an intelligence firm trusted by governments, law enforcement, global corporations, and systemic institutions. We deliver advanced cyber capabilities through a combination of innovative technology and human expertise, perfected by over three decades on the cyber battlefield.

The flagship platform, Zero Day Live, aggregates over proprietary cyber threat intelligence, enabling us to operate at the same speed as the adversary. Our intelligence is delivered finished, actionable and seamlessly orchestrated in overlay, directly into the existing security infrastructure – measurably reducing the risk of a breach to enterprise security architecture by over 50%.

This “Over the Horizon” cyber intelligence on Zero Day Threats coupled with Enterprise Watchlisting can effectively provide the insurance industry with the CYBER TRACKER - equivalent of GPS tracker in a car for motor insurance.

Furthermore, the indexing of the dark web Blackwired provides can deliver precise and independent CYBER RISK MODELING on enterprise risk for UNDERWRITING SUPPORT.

DISCLAIMER

This Document has been prepared by Blackwired Pte Ltd and its affiliates (collectively “BLACKWIRED”) and does not constitute research advice or recommendation.

Nothing in this Document is prepared in relation to your particular circumstances, and before taking any action you should consult technical, legal and other advisors as appropriate. By accepting and using this Document, you are deemed to be represent and warrant to BLACKWIRED that you are able to make your own evaluation of its contents and that you are not relying on BLACKWIRED for advice or recommendations.

This Document is for discussion purposes only and is incomplete without reference to, and should be viewed solely in conjunction with, the oral briefing provided by BLACKWIRED.

This Document and all information and opinions in it are the property of BLACKWIRED. You may not use any portion of this Document except for your personal use, and you may not otherwise distribute or disclose any portion of this Document to a third party without the prior written authorization of BLACKWIRED.

This Document does not constitute a commitment by any BLACKWIRED entity to provide any other services.