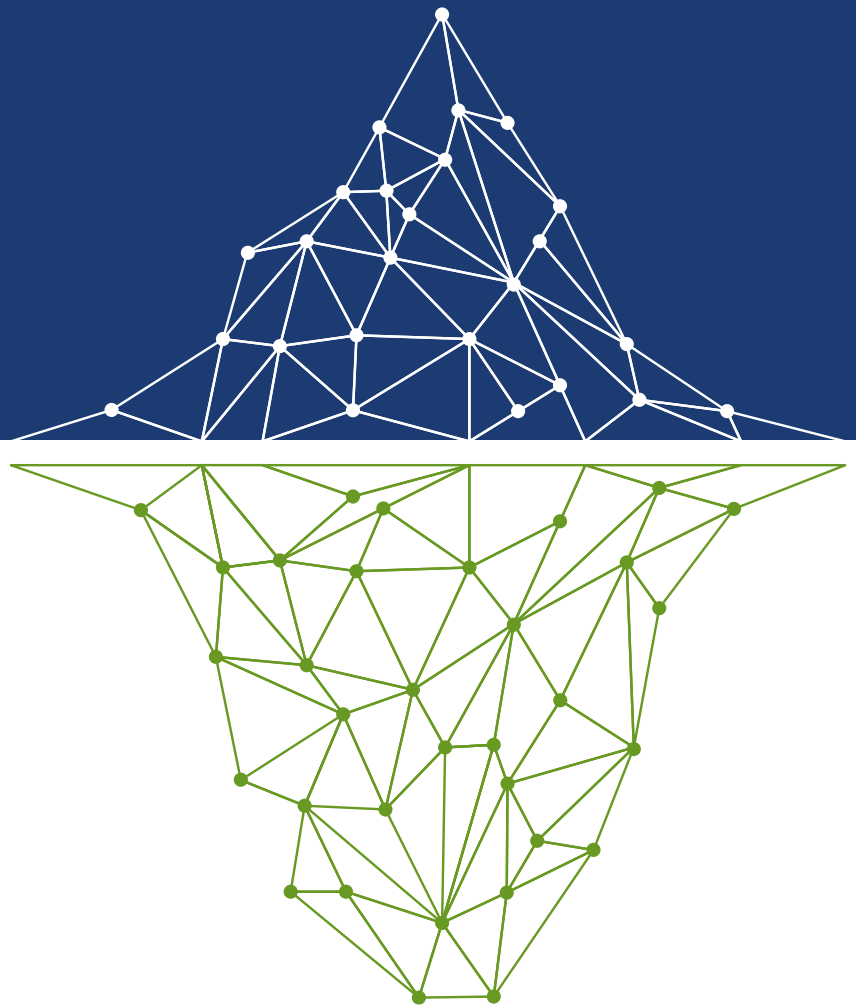
DARKIVORE

Disarm Cyberthreats at the Source



Use Cases

// SUCCESS STORY : AUSTRALIAN SCHOOL

IMPERSONATION, IDENTITY THEFT, CYBERBULLYING

PROBLEM

1. A group of students at an Australian school created TikTok videos impersonating teachers and classmates as a prank.
2. The situation escalated into a cyberbullying campaign, with fake profiles spreading misinformation.
3. Cybercriminals exploited the chaos by creating fraudulent websites to steal personal data from parents and users.
4. The school struggled to manage the growing digital threats as traditional reporting methods were ineffective.

ACTION PLAN

Darkivore took control of the situation – stopping it before it worsened:

1. **Tracked impersonation attempts** and identified fake accounts in real time.
2. **Took down fraudulent websites** and removed malicious content from social media.
3. **Dismantled coordinated harassment campaigns** before they could escalate further.

RESULTS

1. Darkivore took down:
    - 35 fake TikTok accounts
    - 1 fake Instagram account
    - 3 fake websites
1. The school regained control over its digital presence.
2. Students and teachers felt safe to engage both online and in school once again

// SUCCESS STORY : LARGE MULTI-REGIONAL BANK

SOCMINT & ANTI-PHISHING CHALLENGE

PROBLEM

1. The Bank's customers were affected by external fraud attempts through Phishing and Social Media Scam attacks.
2. Executives were suffering from Identity Theft.
3. The customer brand and digital assets were facing reputational damage.
4. Sensitive data was divulged through unintentional leakage.
5. SOC, SIEM, EDR, DLP, NGFW, Pen Tests etc.. Were not pre-emptive enough.

ACTION PLAN

1. Took a proactive approach to enhance company security instead of simply reacting to attacks.
2. Implemented round-the-clock scanning of the surface, deep, and dark web
3. Provided customers with a real-time platform to :
   - Continuously monitor brand's digital footprint on all social media platforms
   - Track usage of brand domain & trade name on various platforms
   - Monitor the online exposure of key personnel

RESULTS

- **Take down of :**
  +9,000 fake pages on Social Media
  +1,500 malicious sites
  +25 rogue Mobile Application detected
- **Deactivation of** +500 fake WhatsApp groups & malicious members
- **Detected & Alerted customers for deactivation of** +2,500 Credit Card leaked
- **Reduced** malicious activities by 99% over 2 years time
- Provided regular weekly & monthly reports that included quantitative analysis of cyber threats and risks.

// SUCCESS STORY : LARGE MULTI-REGIONAL HEALTHCARE COMPANY

MALWARE DARK WEB DATA LEAKAGE

PROBLEM

1. Customers and Dev-Ops employee's data was compromised and sold on the dark/deep web.
2. Many password stuffing, and illegitimate access were detected on their platforms & VPN/PAM.
3. Initial Forensic investigations conducted by 3rd parties showed no sign of customer environment compromise.
4. Still their operations and online platforms were dramatically affected.
5. Cybersecurity teams were confused and overwhelmed.

ACTION PLAN

DARKIVORE

1. **24/7 scanned** the surface, deep and dark web.
2. **Analyzed** the data leakage : Malware installed on employees and end user's personal device that logs user credentials, outside the company's environment.
3. **Detected & Alerted** our client of the compromised users.

RESULTS

- Malware harvested other credentials (personal email & social media accounts) and was not targeting the company specifically.
- Data Leak took place outside the organization environment , company was relieved by the news.
- Client enforced remote access policies to protect their technical employees, changed their credentials immediately.
- Client informed their customers to change their credentials and alerted them about the attack targeting their personal devices.

// DARKIVORE COMPARISON

FEATURES	DARKIVORE	SOCRadar	DARKTRACE	ZEROFOX	PHISHLABS	UpGuard	Blueliv.
Phishing Domain Detection	✓	✓	Limited	✓	Limited (newly created domains)	⊘	✓
Data Leakage (Deep and Darkweb Scavenging)	✓	✓	⊘	✓	✓	Limited to credential compilations	✓
Subdomain Spoofing / Defacement Whaling / Online Forms	✓	Limited	⊘	✓	✓	⊘	⊘
Social Media Coverage	✓	⊘	⊘	✓	Limited local and regional social media presence	⊘	Limited Focused on official references, lack of regional social media.
Unlimited Takedown	✓	Limited Cost/Takedown	⊘	Limited Cost/Takedown	Limited Response Time and Frequency latency	⊘	Limited No takedown service specified
Trademark and Copyright (for e-Market Places)	✓	Limited to DarkWeb marketplaces	⊘	✓	Limited to darkweb marketplaces	⊘	Limited to Social media
Mobile Rogue Apps	✓	✓	⊘	✓	Limited Direct monitoring of official app stores	⊘	✓
Attack Surface Management	✓	✓	✓	✓	Limited	✓	⊘

Let's talk.

Corporate Office
4/9 Fitzpatrick St,
Revesby NSW 2212

Phone
1300 010 113

Online
Email: info@intelus.com.au
Website: www.intelus.com.au

intelus