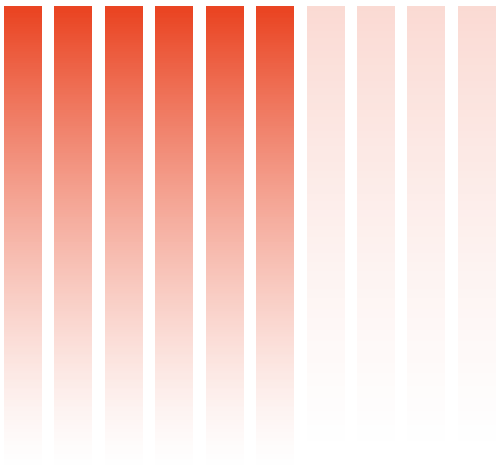
SEARCHLIGHT. CYBER

COMBATING INSIDER THREAT WITH DARK WEB INTELLIGENCE

THE CHALLENGE



60 PERCENT OF ORGANIZATIONS HAVE EXPERIENCED ONE OR MORE INSIDER THREAT-RELATED INCIDENTS IN THE PAST YEAR.

Insider threats - a malicious employee, contractor, or third party with privileged access - are a security team's worst nightmare. They sit inside the perimeter, they need to have access to sensitive documents and data to perform their roles, and they have unique power to undermine the security of the organization from within.

According to recent research, 60 percent of organizations have experienced one or more insider threat-related incidents in the past year.[1] Indeed, we regularly observe evidence of insider threats on the dark web. Employees post on forums to attract buyers in the cybercriminal community, cybercriminals try to recruit insiders, and those that have already done so advertise their "innys" for other cybercriminals to use for a fee.

Counterintuitively, sometimes the best indicators of a compromised insider can be found in signals outside of the company network. This activity on the dark web - where cybercriminals believe they can act with impunity - provides security teams with an opportunity to identify and stop insider threats.

This report looks at how warning signs of a malicious insider can be used to inform internal investigations based on intelligence on who the compromised employee is, the access they have, and their motivation.

[1] https://www.securitymagazine.com/articles/98879-over-half-of-organizations-experienced-an-insider-threat-in-2022

FIVE WAYS YOU CAN SPOT INSIDER THREAT OUTSIDE OF YOUR NETWORK

1

MONITOR DARK WEB FORUMS FOR MALICIOUS INSIDERS

Security teams should be monitoring for employees using dark web networks such as The Onion Router (Tor) to communicate with the wider cybercriminal underworld or to leak data.

Malicious insiders using the dark web are more likely to be technically capable, serious about their malicious intentions, and better able to access the tools they need to execute their attack. They should therefore be seen as a high-priority threat.

By monitoring dark web forums, organizations can identify indicators that it is their organization being targeted, such as their brand name being used, leaked company data, or corporate email addresses. They can also gather intelligence that could help them in their investigation of a malicious insider, such as employee contact details or an indicator of which department the employee is in.

Typically, we observe malicious insiders using dark web hacking forums to:

- Advertise their employment at a company to attract cybercriminals interested in paying for insider threat services.
- Offer initial access into a corporate environment for cybercriminals to bid on.
- Sell data or intellectual property that the malicious insider has already stolen from the company.
- Ask for guidance from cybercriminals on how they can exploit the company.
- Buy malware or other tools to execute an attack on the organization.

> MALICIOUS INSIDERS USING THE DARK WEB ARE MORE LIKELY TO BE TECHNICALLY CAPABLE, SERIOUS ABOUT THEIR MALICIOUS INTENTIONS, AND BETTER ABLE TO ACCESS THE TOOLS THEY NEED.

I have physical access to bank computers that can pull up all customer into, wire funds from any customer, make changes to account, etc. I can get task manager process list, av/edr versions etc.

Need someone to assist in custom designed malware for intrusion to covert use the software to make changes to bank account. PM with xmpp detail if you are expert.

Hello i'm looking for the following and would appreciate some answers, been a while since I was in the game :)

Best R.A.T at the moment? Paid or free doesn't matter. Been looking closer at Quasar and like the simple layout, looks stable.

I also look for a stable vendor who can deliver FUD crypt as often as needed, Ofc I will be paying.

Looking for someone who can hook me up with a Word/ Excel exploit $$$.

All in one would be the best :) if you got the things I need and some answers DM me :)

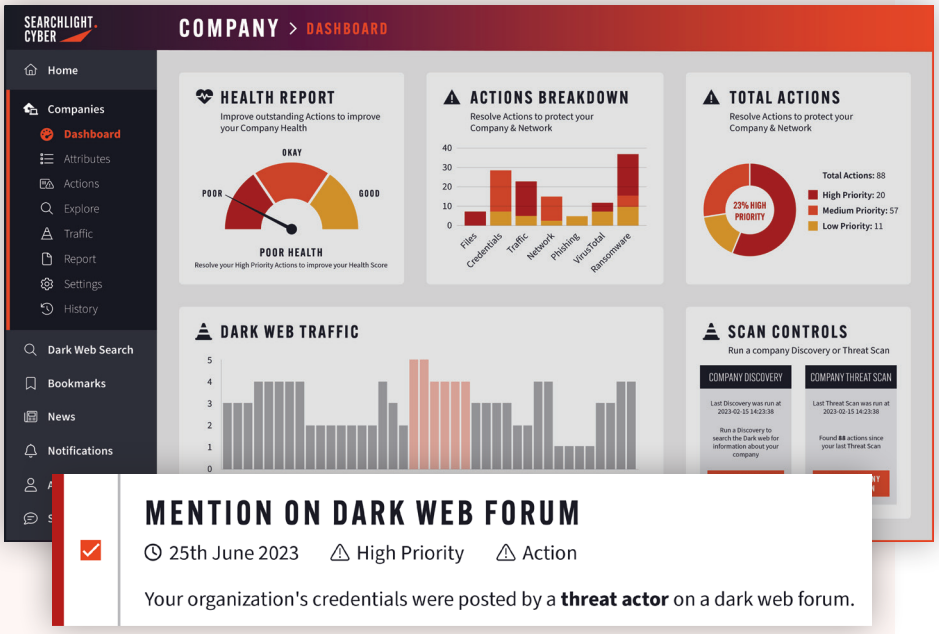
These two posts are real examples from a malicious insider who was requesting tools from the cybercriminal community to execute their attacks on their employer. RAT refers to Remote Access Trojan, and FUD means "fully undetectable".

HOW TO COMBAT INSIDER THREAT WITH SEARCHLIGHT CYBER

Searchlight Cyber continuously monitors dark web marketplaces and forums to help you spot the earliest warning signs of an attack, including threats from employees undermining the security of their organization and cybercriminals soliciting insider information.

MONITOR FOR DARK WEB MENTIONS

Just enter your organization's attributes, such as domains, IP addresses, and employee credentials, and Searchlight will automatically scan them against over 8 million dark and deep web records. Searchlight then categorizes and proactively alerts you to imminent threats against your organization – saving your analysts valuable time.



2 MONITOR FOR RECRUITMENT POSTS TARGETING YOUR EMPLOYEES

Organizations should also be monitoring the dark web for cybercriminals who are stalking the underworld of the internet to recruit insiders for their operations. Cybercriminals routinely post adverts on dark web forums offering handsome payouts to employees who can provide them with privileged access. This is a major source of insider threat as, according to the Verizon 2023 Data Breach Investigation Report, 89 percent of malicious employees are motivated by financial gain.[2]

> CYBERCRIMINALS ROUTINELY POST ADVERTS ON DARK WEB FORUMS OFFERING HANDSOME PAYOUTS TO EMPLOYEES WHO CAN PROVIDE THEM WITH PRIVILEGED ACCESS.

****** insider needed. Have full access to a dead person account. Dormant 6 months+. Have everything except the physical card. Have original ID. Access to online and telephone banking. Have full victim personal details.

Just need insider to verify ID and we can cashout 300k in one day.

Message me here, or telegram.

A cybercriminal on the dark web forum Exploit tries to recruit a bank insider with access to the account of a deceased individual, in order to commit fraud.

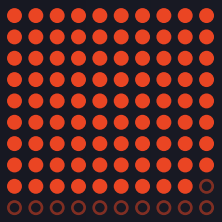
For example, in the post above the target bank was named (redacted by us), which means that this intelligence could have been used by the organization to monitor for suspicious account activity or malicious employee behavior. At the very least, the bank's cybersecurity team should create a standing intelligence requirement to monitor for interactions with the post.

A proactive cybersecurity team could use this post to:

- Pivot on the alias of the cybercriminal to determine the capability (and therefore risk) of the perpetrator.
- Monitor for responses and assess if their employees are engaging.
- Use the information the cybercriminal provides on their scheme to run an intelligence-led investigation into whether this type of fraud is taking place within their business.

[2] https://www.verizon.com/business/resources/reports/dbir/

INSIDER THREAT IN NUMBERS



89% OF MALICIOUS EMPLOYEES ARE MOTIVATED BY **FINANCIAL GAIN**[3]

44% INCREASE IN THE NUMBER OF **INSIDER INCIDENTS** FROM 2020-22[4]

INTERNAL ACTORS ARE RESPONSIBLE FOR **19%** OF **ALL BREACHES**[5]

$15.38M WAS THE TOTAL **AVERAGE COST** OF AN INSIDER THREAT IN 2022[6]

TAKE ACTION RIGHT AWAY WITH OUR NO-INSTALL PLATFORM

- ADD YOUR CREDENTIALS
- GET NOTIFIED OF EMERGING THREATS
- TAKE PRE-EMPTIVE ACTION TO STOP CYBER ATTACKS

[3] https://www.verizon.com/business/resources/reports/dbir/
[4] https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats
[5] https://www.verizon.com/business/resources/reports/dbir/
[6] https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats

3

MONITOR TOR TRAFFIC TO AND FROM THE COMPANY NETWORK

Traffic between Tor and the company network can also provide an early warning sign of insider threats.

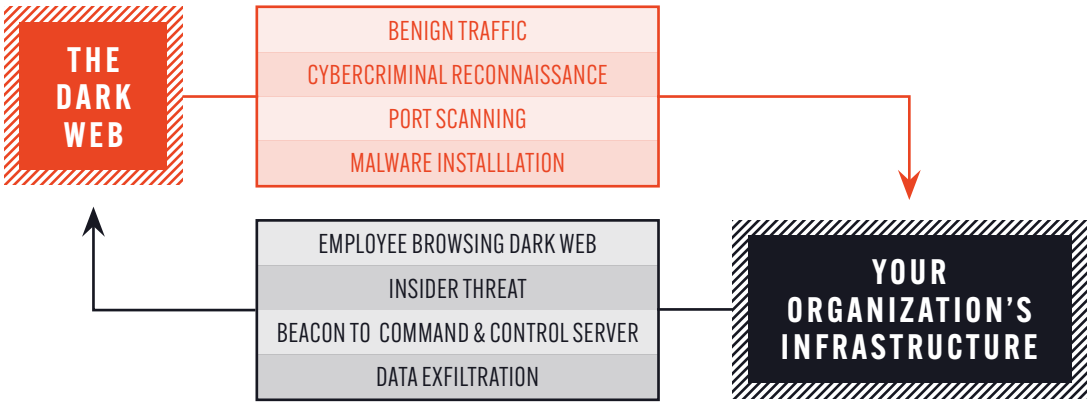
Many large organizations will have traffic coming from Tor to their network, especially public facing infrastructure like their website. This can be benign traffic, where people are simply viewing the website from the dark web, but it is certainly worth monitoring for signs of cybercriminal reconnaissance. For example, dark web traffic to non-browsable web content like VPN portals can indicate that criminals are scanning ports for vulnerabilities. Monitoring for anomalous traffic activity, such as a large number of connections, or inconsistencies in data request vs response can help security teams to identify if their network is being probed or attacked by cybercriminals.

However, connections from the company network to the Tor network are a very reliable data point for discovering insider threat because - in most organizations - there is virtually no good reason why an employee would be connecting to the dark web.

Traffic going from an organization's network to the dark web usually indicates one of only a few possibilities and each of these justifies immediate investigation from the security team:

- An employee is engaging in illegal activity on the dark web, which is potentially putting the company at risk.
- An employee is deliberately engaging with cybercriminals through the dark web, which could include sharing data or providing access to the network.
- The network has already been compromised and the traffic leaving the corporate network is a beacon calling back to a command and control server.

NETWORK TRAFFIC TO AND FROM TOR



HOW TO COMBAT INSIDER THREAT WITH SEARCHLIGHT CYBER

SPOT SUSPICIOUS TOR TRAFFIC TO AND FROM YOUR NETWORK

A sudden surge in Tor traffic to your network is a clear warning sign that your organization may soon be under attack. Searchlight's proprietary dark web traffic monitoring technology offers automated alerts for detecting this pre-attack activity, empowering security teams to identify the earliest indicators of data exfiltration.

Date	Type	Host	IP Address	Port	Sum of Data-In	Sum of Data-Out	Total Connections
2023-06-19 14:56:01 UTC	Outgoing	yourdomain.com	148.61.6.9	80	-	-	-
2023-06-20 17:12:23 UTC	Outgoing	yourdomain.com	148.61.6.9	80	-	-	-
2023-06-20 21:03:51 UTC	Incoming	yourdomain.com	148.61.6.9	523	280kb	2.6gb	7,432
2023-06-21 04:41:42 UTC	Outgoing	yourdomain.com	13.57.92.51	80	-	-	-
2023-06-22 14:38:20 UTC	Incoming	yourdomain.com	13.57.92.51	523	1.1gb	3.2gb	11,412

BENEFITS: DARK WEB TRAFFIC MONITORING FOR YOUR ORGANIZATION

- AGENTLESS DEPLOYMENT WITH OUR OUTSIDE-IN APPROACH TO DATA COLLECTION
- DEFEND AGAINST MALWARE INSTALLATION AND DATA EXFILTRATION
- DETECT CRIMINAL RECONNAISSANCE AND INSIDER THREATS
- DETECT ANOMALIES IN DARK WEB TRAFFIC LOGS, SUCH AS LARGE DOWN OR UPLOADS

4

MONITOR CLEAR AND DEEP WEB HACKING SITES

Organizations should also be monitoring for signals of insider threat on clear and deep web hacking websites, as well as messaging services such as Telegram. These sites are more accessible for users with less technical capability so are popular for malicious insiders conducting "lower level" cybercrime such as fraud. However, more serious cybercriminal operations also use these sites to find malicious insiders who might not frequent the usual dark web forums where they operate.[7]

Clear web sites are those that can be accessed via a regular browser, where individuals quite brazenly discuss cybercriminal activity. Meanwhile, deep web hacking forums refer to the likes of BreachForums or Cracked - sites that you are able to visit via regular browsers but which require credentials to post, creating a barrier for non-criminals.

> Looking for US Bank insiders who have US company bank details (we are mostly looking for dormant accounts with lots of money in them and lots of activity prior to the account becoming dormant). You will need to have access to the bank statement where you will have a reference number of the micro-deposit so that we do so we can pull money out of it, we can talk more details in PM :)

Insider recruitment post from the deep web hacking forum, Cracked.

The messaging app Telegram is particularly popular for advertising and recruiting malicious insiders. For example, the messages taken from Telegram below are advertising insiders conducting fraud at insurance companies, bank employees who can undertake bank transfers, and SIM-swapping at Telecommunication companies.

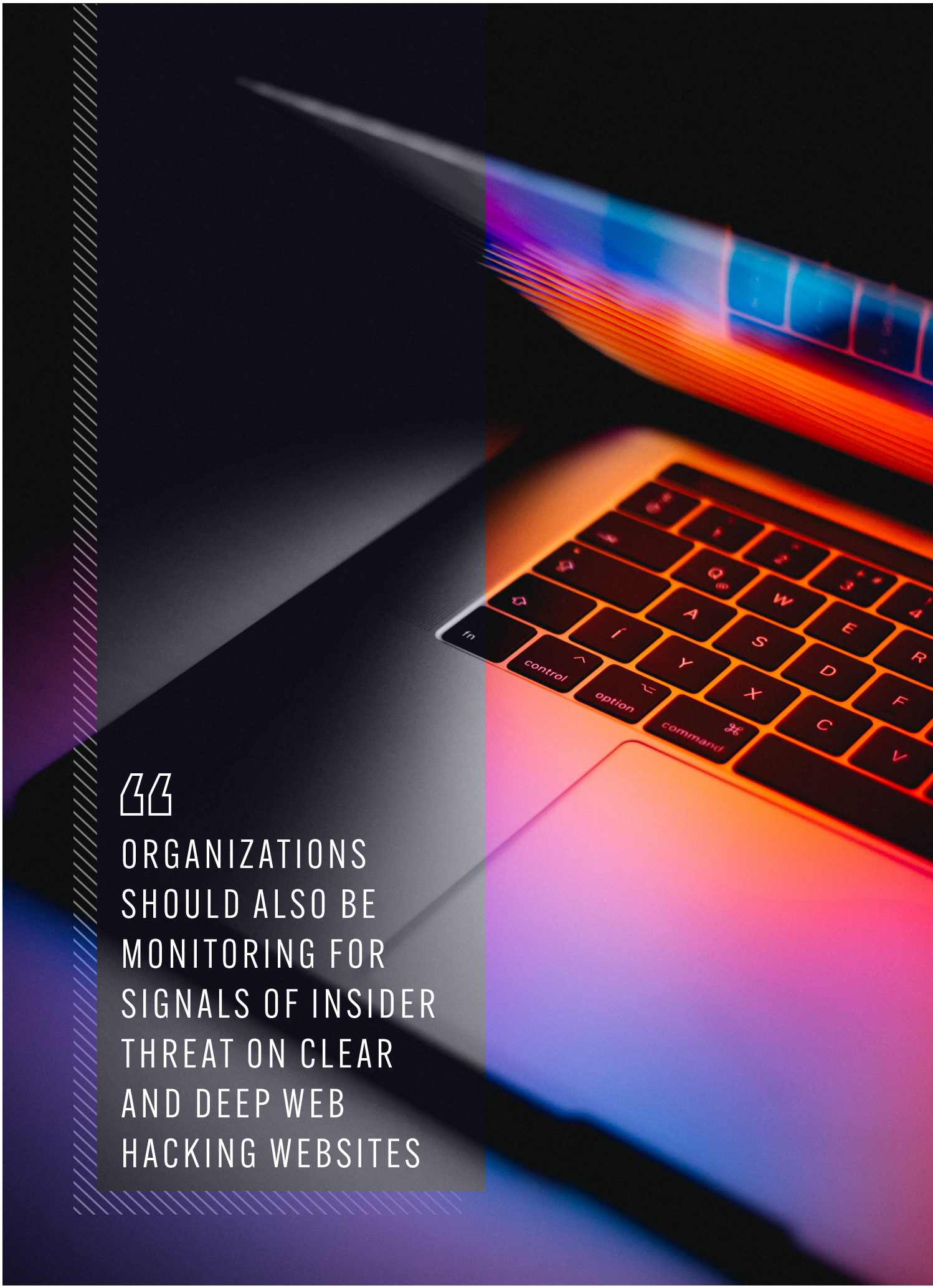
> T-mobile inny is up
> info needed
>
> - phone number
> - sim picture

> PC financial insider that
> can do wires up to 300k..
> 60/40 split pm

> Who needs auto car insurance!!
> Registered policy # by insider reason to why it works at service ontario.
> Register your car now with a G1 G2 G or get plates.
> PM with any questions.

Malicious insiders are sometimes nicknamed "innys" on Telegram and hacking forums.

[7] https://www.slcyber.io/cybercrime-on-telegram-a-connection-to-the-dark-web/



> ORGANIZATIONS SHOULD ALSO BE MONITORING FOR SIGNALS OF INSIDER THREAT ON CLEAR AND DEEP WEB HACKING WEBSITES

5

BUILD THREAT MODELS, RUN TABLE TOP EXERCISES, AND THREAT HUNT

Beyond identifying incidents that specifically relate to them, monitoring externally for insider threats can help security teams to build out their intelligence and improve their readiness for attacks.

Many security teams have to consider malicious insiders with privileged access as part of their threat model and collect intelligence on the hypothesis that they have an insider threat.

Standing intelligence requirements for this threat model could include:

- Identifying the assets that malicious insiders are likely to target.
- Identifying areas of weakness - such as uncontrolled access - and possible countermeasures.
- Identifying the adversaries that are likely to target their sector and how they might communicate and use insiders.
- Identifying potential trigger events for an attack - such as employee layoffs.
- Learning from previous incidents and public reporting of insider threats and leveraging that understanding to inform defense and detection capabilities.

Meanwhile, threat hunting teams concerned about insider threat can proactively use the intelligence gathered by monitoring the dark web to investigate on the assumption that the insider is within their business. For example, they could pivot on the profile of an insider advertising their access within an organization to identify whether this is one of their employees. Alternatively, threat hunters could pivot on the profiles of the cybercriminals that interact with the post to identify their capabilities based on their wider dark web activity.

Even if companies aren't resourced to conduct threat hunts, the dark web posts could be leveraged as inspiration for table top exercises. For example, taking the scenario: "what is the employee in this post was within our business? How would we respond to this incident?" Having a predefined game plan in place can have a major impact once a real-life threat is identified.

> MANY SECURITY TEAMS HAVE TO CONSIDER MALICIOUS INSIDERS WITH PRIVILEGED ACCESS AS PART OF THEIR THREAT MODEL.

HOW TO COMBAT INSIDER THREAT WITH SEARCHLIGHT CYBER

EMPOWER YOUR THREAT HUNTING TEAM

Give your cyber teams access to previously unobtainable live activity and over 15 years of archived dark web data. Our digital archive of the dark web can easily be searched and filtered – without the conventional dangers tied to accessing the dark web. This includes access to deleted posts, such as the sale of sensitive information, that are deleted in an attempt to hide them from sight.

SELLING BANK OFFICE ACCESS

ThreatActor posting on Forum at 28 Jun 2023 20:30

Electrician with access to bank's computers and server room.

RECRUIT INSIDERS

ThreatActor posting on Forum at 15 Aug 2023 17:10

Employees at telecomm, gaming, call center or server hosts send a DM and we will respond!!!

EARN $$$ IN BITCOINS

ThreatActor posting on Forum at 05 Jul 2023 11:46

Provide us login and password to RDP, VPN, or corp email.

LOOKING FOR BANK INSIDERS

ThreatActor posting on Forum at 14 Jun 2023 14:23

Need bank or ATM insider to work with and make big money.

LOOKING FOR INSIDER FRANCE

ThreatActor posting on Forum at 02 May 2023 21:55

Gov, insurance, public health care, national database for - pay well with escrow

- EASILY SEARCH AND PIVOT ON DARK WEB THREATS AND ACTORS
- CREATE ACTOR ACTIVITY ALERTS TO HUNT DOWN SUSPECTED INSIDERS
- SEARCH LIVE AND HISTORIC DATA, INCLUDING POSTS THAT HAVE BEEN DELETED
- SECURELY ACCESS TOR AND I2P FROM YOUR BROWSER USING OUR STEALTH BROWSER

SEARCHLIGHT CYBER

SEARCHLIGHT CYBER HELPS ORGANIZATIONS SAVE TIME AND MONEY BY SPOTTING THE FIRST WARNING SIGNS OF AN ATTACK.

★★★★★

"The system provided by Searchlight Cyber DarkIQ makes our SOC team more efficient in threat hunting and breach investigations."

HEAD OF CONSULTING (SOURCE: GARTNER PEER INSIGHTS)

SCAN THE QR CODE TO BOOK YOUR FREE DEMO TODAY OR VISIT **WWW.SLCYBER.IO** TO FIND OUT MORE.

UK HEADQUARTERS
Suite 63, Pure Offices,
1 Port Way, Port Solent,
Portsmouth PO6 4TY
United Kingdom

US HEADQUARTERS
900 16th Street NW,
Suite 450, Washington,
DC 20006
United States