The Dark Web: A Treasure Trove of Actionable Threat Intelligence

*Presented by Q6 Cyber and ASMGi*

Feb 20, 2019
Today’s Webinar
*The Dark Web: A Treasure Trove of Actionable Threat Intelligence*

• What is the “Digital Underground”? The “Dark Web”? The “Deep Web”?  
• Who are the threat actors on the “Underground” targeting financial institutions?  
• How can I collect targeted & actionable intelligence on the “Underground”?  
• How do leading organizations leverage such intelligence to combat cybercrime and fraud?  
• What can institutions do to eliminate these threats?
ASMGi is …

– Global Technology Services and Consulting company focused on solutions that provide immediate positive impact on your business

– We deliver IT, Software and Cyber Security solutions from our headquarters in Cleveland, OH. We help our customers Plan, Manage and Execute:

  • Strong programs as a foundation to meet compliance requirements as well as foster best practices across the enterprise
  • Best-in-Class platforms and tools to drive adoption and shorten time to value
  • A security eco-system model to ensure tools work together
  • An execution plans that are designed to achieve results:
    • ONETeam “XaaS” capabilities to ensure you maximize adoption – Benefits without the Burden!
    • “Fill the gap” approach to leverage your existing resources and complement/supplement where needed
  • Action = Results -> Orchestrated Action = Great Results!
The Dark Web...

I am excited about today’s webinar!

– Q6 is about providing Actionable Information

– Most of us know the Dark Web exists, but don’t know what it looks like and how it works

– It’s not a matter of if, but when your data is compromised .... Is it possible to minimize or eliminate fraud even after your data makes it to the dark web?

Please welcome Eli Dominitz, CEO of Q6 Cyber
Today’s Guest Speaker

Eli Dominitz
CEO, Q6 Cyber

info@q6cyber.com

www.q6cyber.com
What Is The Digital “Underground”? 

- Online sites, marketplaces, communities, and forums where hackers, fraudsters, and cybercriminals operate and interact.
- Malware networks and infrastructure.
- Includes the “DarkNet” or “DeepWeb” - anonymous and largely inaccessible.
Monitoring The Digital Underground to Provide Targeted & Actionable Threat Intelligence
Live Demo
Large Bank Case Study (30 days)

- 400,000 compromised payment cards identified
- 554 compromised merchant accounts and/or POS devices identified
- $1.2 Million potential fraud losses prevented
- 498 compromised employee credentials identified
- 7 new merchant breaches discovered
- 2 TTP bulletins (e.g., SIM Card Duplication / Hijacking)
- 7 potential fraud losses prevented
Delivering Substantial ROI

$335,100 DIRECT SAVINGS
5.8x ROI

$134,040 INDIRECT SAVINGS
2.3x ROI

$335,100 REVENUE UPSIDE
5.8x ROI

1,117 CARDS STILL ACTIVE
We detected 1,597 compromised payment cards of which 1,117 are still active with no fraud committed yet.

PREVENTION
Bank can now take proactive action to prevent fraud losses on these cards (i.e., replace cards or enhance monitoring).

DIRECT SAVINGS: $335,100
1,117 cards x $300 average loss per card (based on the low end of industry average) = $335,100.

COSTS OF HANDLING CLAIMS
Internal operational costs of handling fraud claims is on average $120 per case.

AVOIDING FRAUD CLAIMS
Bank now avoids fraud claims on 1,117 cards detected.

INDIRECT SAVINGS: $134,040
1,117 cards x $120 average cost = $134,040.

According to Visa, the secondary effects of fraud cost issuers an amount equal to direct fraud losses.

CUSTOMER ATTRITION
6-23% of consumers switch financial institutions as a result of fraud.

REduced CARD USAGE
32-69% of consumers choose alternative payment method over credit/debit card following a fraud incident.

BRAND IMPACT
10-33% of consumers report being “somewhat” or “very” unhappy with the treatment from their financial institutions after fraud incident.
Next in our Cyber Webinar Series

Cyber Security webinar series: *Quantifying Cyber Risk – Real or Hocus Pocus?*

Presented by ASMGi and Tower Street, on Thursday February 28, 1PM ET

**What we will cover:**

- The pressing need for companies to quantify their cyber risk exposures in dollar terms.
- The pressing need for companies to quantitate their cyber risk exposures in dollar terms.
- The limitations of current qualitative measurement methodologies used.
- We will investigate the application of quantitative measurement for smarter budgeting, clarity of balance sheet impact and insurance decisions."
- Qualitative Measurement (current methodology): Insurance impact = “One size fits all”; price in-transparency; risk capital limiting
- Quantitative Measurement: Insurance impact = “Fit for purpose”; value & price transparency; risk capital expanding

*Visit the [www.ASMGi.com](http://www.ASMGi.com) Resources page to sign up*
Thank You