

Eli Dominitz, CEO
eli@q6cyber.com

MIAMI | TEL AVIV | WWW.Q6CYBER.COM

Latest Trends in Cybersecurity



THE GOOD GUYS ARE:

- ❖ Collecting and integrating actionable threat intelligence
- ❖ Implementing cloud security
- ❖ Addressing third-party risk
- ❖ Protecting information at the database and data element level
- ❖ Upgrading security awareness training



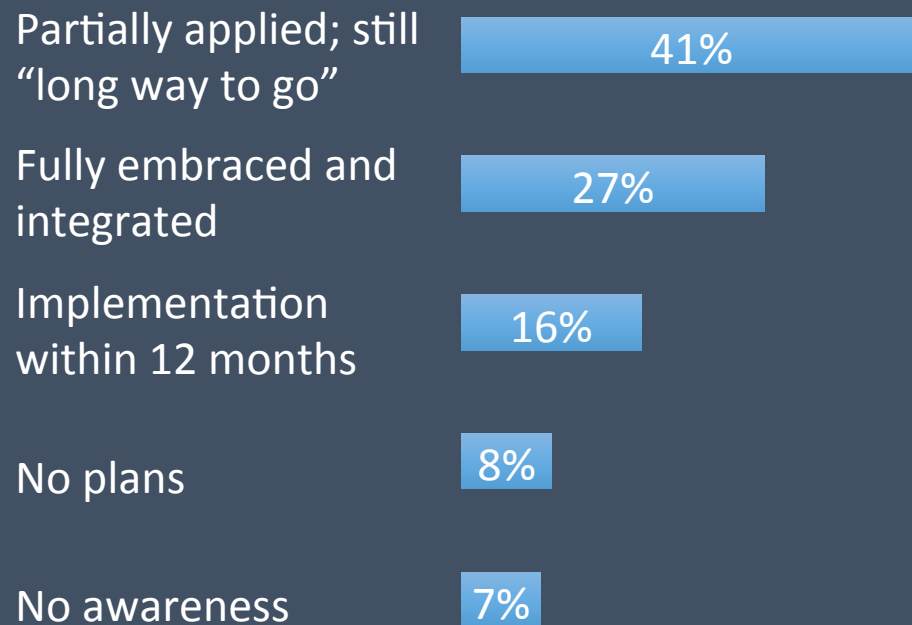
THE BAD GUYS ARE:

- ❖ “Commercializing” their skills
- ❖ Intensifying and evolving ransomware attacks
- ❖ “Doubling down” on social engineering
- ❖ Escalating mobile attacks
- ❖ Pursuing “softer” targets

Threat Intelligence – Transforming Cybersecurity Models



Awareness and Consumption of Cyber Threat Intelligence is Growing...



...As Organizations Seek to Transform their Cybersecurity Operations

- ✓ From reactive to proactive
- ✓ Reduce overwhelming alerts
- ✓ Prioritize relevant, targeted threats
- ✓ Integrate intelligence into security systems
- ✓ Information sharing and cooperation



EXAMPLE



Actionable Threat Intelligence – Detecting Breaches Ex Post Facto and Reducing Fraud

Dumps

Bin	Carr.	Type	CD	Bank	Country	Base	Qty	Price		
[REDACTED]	101	VISA PLATINUM	DEBIT	[REDACTED]	UNITED STATES	WORLD_BIG_UPDATE	36	\$18.00	<input type="text" value="0"/>	↑ ↓ To cart
[REDACTED]	101	VISA CLASSIC	DEBIT	[REDACTED]	UNITED STATES	WORLD_BIG_UPDATE	2	\$13.00	<input type="text" value="0"/>	↑ ↓ To cart
[REDACTED]	101	VISA CLASSIC	DEBIT	[REDACTED]	UNITED STATES	WORLD_BIG_UPDATE	1	\$13.00	<input type="text" value="0"/>	↑ ↓ To cart
[REDACTED]	101	VISA PLATINUM	DEBIT	[REDACTED]	UNITED STATES	HOT_MARCH_UPDATE	33	\$18.00	<input type="text" value="0"/>	↑ ↓ To cart
[REDACTED]	101	VISA PLATINUM	DEBIT	[REDACTED]	UNITED STATES	HOT_MARCH_UPDATE	17	\$18.00	<input type="text" value="0"/>	↑ ↓ To cart
[REDACTED]	101	VISA CLASSIC	DEBIT	[REDACTED]	UNITED STATES	HOT_MARCH_UPDATE	1	\$13.00	<input type="text" value="0"/>	↑ ↓ To cart
[REDACTED]	101	VISA CLASSIC	DEBIT	[REDACTED]	UNITED STATES	HOT_MARCH_UPDATE	12	\$13.00	<input type="text" value="0"/>	↑ ↓ To cart
[REDACTED]	101	VISA PLATINUM	DEBIT	[REDACTED]	UNITED STATES	HOT_MARCH_UPDATE	2	\$18.00	<input type="text" value="0"/>	↑ ↓ To cart

Cloud Security: Exponential Adoption Fueling Cyber Attacks



87% of organizations are using public cloud



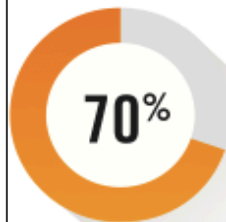
\$127 Billion

Size of global cloud computing services market by 2017, representing 35% CAGR

YEAR-OVER-YEAR COMPARISONS

CLOUD ENVIRONMENTS

ON-PREMISES DATA CENTER



App Attack
45% INCREASE



Suspicious Activity
36% INCREASE



Brute Force
27% INCREASE



Suspicious Activity
3% INCREASE



Trojan
1% INCREASE



App Attack
6% INCREASE

Third Party Risk – A Complex Challenge














Third parties are implicated in
20-40% of security breaches



70% of attacks with a known motive have a secondary victim



The “Commercialization” of Cyber Crime – Example of Online Marketplace

	Skimmer & Green Started by spongebob,	Replies: 2 Views: 372	darkknight67 Yesterday, 08:32 AM >
	botnet and banking botnet set up, Rat keyloggers trojans crypters... Started by parahack,	Replies: 6 Views: 905	contatowork Yesterday, 03:49 AM >
	Paypal account needed Started by slidi,	Replies: 2 Views: 137	dr34ml0ve 08-16-2015, 06:44 PM >
	New rdp Started by selltool,	Replies: 1 Views: 382	medo_trable 08-16-2015, 11:24 AM >
	Simple Scampage Full info Started by Garan9,	Replies: 0 Views: 37	Garan9 08-15-2015, 08:25 PM >
	paypal checker online Started by medo_trable,	Replies: 0 Views: 107	medo_trable 08-13-2015, 03:06 PM >
	western union money transfer hack Started by das50505, 1 2 3 ... 15	★★★★★ Replies: 146 Views: 17,539	fahadkamal 08-13-2015, 12:06 PM >
	Carding tools with good customer service Started by gumical1,	Replies: 3 Views: 1,074	fahadkamal 08-13-2015, 11:54 AM >
	Buy scanned ID of identity and passport Started by ma4vip,	Replies: 6 Views: 399	tingtoong 08-12-2015, 09:06 PM >
	[service] scan bank statement,cvv,drive license,passport... All state usa Started by tingtoong,	Replies: 0 Views: 40	tingtoong 08-12-2015, 09:05 PM >
	ID/Documentation scans and copies Started by Coricus,	Replies: 1 Views: 87	slizzy010 08-11-2015, 01:29 AM >

The “Commercialization” of Cyber Crime



ACTORS

- ❖ financially driven, organized and sophisticated
- ❖ Geographically diverse
- ❖ Usually disguised in darknets, invitation-only forums, and protected by cryptography



PRODUCTS & SERVICES

- ❖ Stolen records, exploit kits, zero-day vulnerabilities, etc.
- ❖ “Crime as a Service”
- ❖ SaaS models and point-and-click tools with online tutorials
- ❖ Vendor guarantees



PRICING

- ❖ Generally decreasing due to oversupply (e.g., credits cards, DDOS services, botnets)



ACCESS

- ❖ Growing due to proliferation of platforms and technology
- ❖ Offset by increased vetting in more sophisticated marketplaces



Intensifying and Evolving Ransomware Attacks



Ransomware – DD4BC DDOS Extortion Campaign

From: DD4BC Team [<mailto:dd4bcteam@keemail.me>]

Subject: DDOS ATTACK!

Hello,

To introduce ourselves first:

[hXXp://www.coindesk.com/bitcoin-extortion-dd4bc-new-zealand-ddos-attacks](http://www.coindesk.com/bitcoin-extortion-dd4bc-new-zealand-ddos-attacks)

So, it's your turn!

Your sites are going under attack unless you pay 25 Bitcoin. Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps, so don't even bother.

Right now we are running small demonstrative attack on one of your IP's. Don't worry, it will not be hard and will stop in 1 hour. It's just to prove that we are serious.

Fullname: DD4BC Team

Twitter: <https://twitter.com/dd4bc>

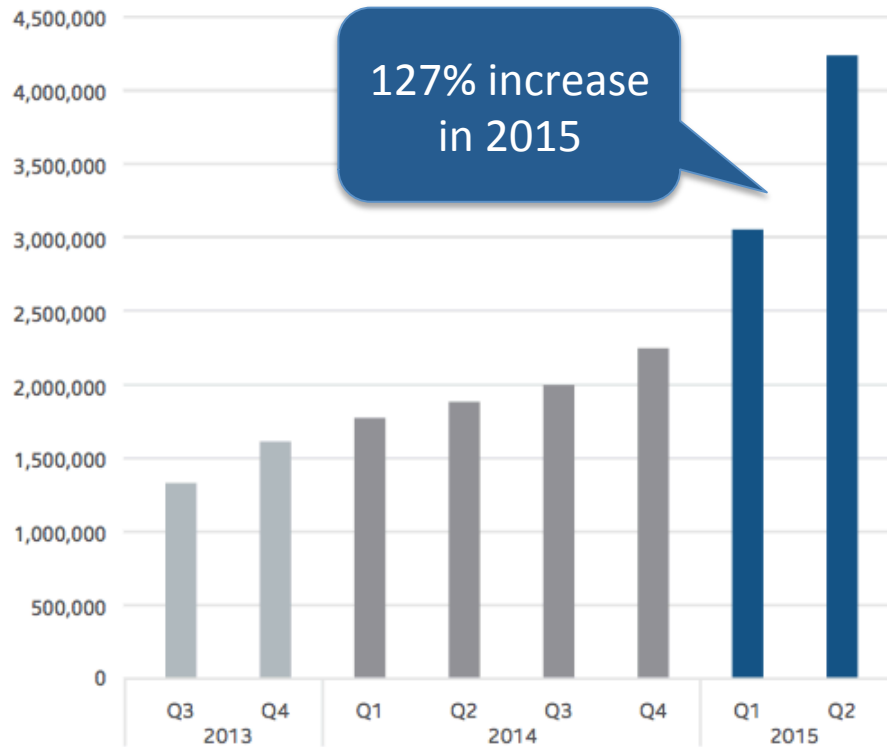


Twitterimage:

Klout: <http://klout.com/dd4bc>

Intensifying and Evolving Ransomware Attacks

Ransomware Samples



- ❖ Increasingly sophisticated - involving DDOS, intellectual property theft, etc.
- ❖ Costs go beyond the ransom fee itself (e.g., network mitigation, legal fees, countermeasures, loss of productivity)



Social Engineering – Same Old Tricks, More Sophisticated Targeting and Application



4-8%

Of social media links are malicious in nature



23%

Of email recipients open phishing messages and 11% click attachments



62%

Increase in data breaches resulting from spear phishing



Thank You!

Eli Dornitz, CEO
eli@q6cyber.com

