Evolution of Hackers and Reverse Incident Response

Alex Holden

Chief Information Security Officer
Hold Security, LLC
@HoldSecurity
Goal: Typical problem, different perspective
Evolution
Hackers – Learning To Be Different

- Learning new things – survival techniques
  - Technologies
  - Language barriers
  - Geopolitical drivers
Hackers – Learning To Make Money

- Sharing knowledge = Innovation
- Business schemes
- Technology innovations
- Payout
Hackers – Learning To Organize

- Gang life ideology
- Structure
- Turf
- Weaknesses

“I’m fighting a holy war against the West… They drive their Rolls Royces and go home to their million-dollar houses, while people here are struggling. I will never harm my fellow Slavs; but America, Europe, and Australia deserve it.”

- aqua (jabberzeus gang)
Modern Actors - Transformation
Modern Actors – Transformation (Take 2)

- Не говорит по-английски
- Semi-educated
- Lazy
- Money-hungry
- Addicted to drugs, alcohol, gambling
Modern Actors – Transformation (Cont’d)

- 99% of hackers fail in their careers
- On the run from the law
- On the run from competition
- On the run from street gangs
Black Market – Specialization

- Break complex processes into small tasks
- Hacker professions
- Marketing
- Community education
Incidents
Breaches
Opportunities
Reverse Incident Response

0110001001110010011001010110000101100011011010000110
010101100100001000000110010011000010111010001100001
Incident Response

Breach

Indicator Of Compromise (IOC)

What data was taken?

Investigation, forensics, regulatory risks

Who? How? Why?

Attributions, risk management
Breach In-The-Making

- **Actors**
  - Targeting
  - Motive

- **Skills**
  - Skill set
  - Orders

- **Data**
  - Useful data
  - Collateral Damage

- **Methods**
  - Technologies
  - Monetizing
Incident Components

- IOC, Logs, Evidence, Data, Investigators, Regulators, Lawyers, Victims, Media.
- Credentials, Financial, System, Blackmail, Partners, Vendors, Customers, Employees.
- Motives, Opportunities, Technologies, Techniques, Relationships.
- Orders, Services, Forums, Chats, Debts, Cashing Out, Collateral Damages.
Reverse Incident

- Creating data connections
- Is it credible?
- Who has it?
- Where did it come from?
- What are the next steps?
Following Actors

- **Profile**
  - Specialties
  - Acquaintances
  - Footprint
  - Locale

- Role
  - Who else has this data
  - Success rates
  - Monetization strategy
Following Data

- Data types
- Locations seen
- Potential full data size
- Sophistication
- Primary purpose
- Residual value

Breach scope
Distribution, intent
Victim profile
Encryption and other defenses
Vectors of abuse
Future abuse
Correlations

- Vectors of compromise
- Black market value
- Link in a chain – other actors
- End goal – monetization, blackmail, etc.
- Similar data
Deep Web IOC To Data Breach

Data → Actors → Monetization → Breach

- **Breach**
  - **Indicator Of Compromise (IOC)**
  - **What data was taken?**
    - Investigation, forensics, regulatory risks
  - **Who? How? Why?**
    - Attributions, risk management

- **Data**
- **Actors**
- **Black Market**
Advice - Learning Process

- Know your enemy
- Understand and classify your data
- Don’t assume that your organization is “hacker-proof”
- Get to know your “circle of friends” — vendors/partners/customers
Advice - Honeypots

- Honeypots are not only systems
  - Components
  - Credentials
  - Features
Advise - Quantitative Analysis

- How much of your data is transferred?
- What is normal? What is not?
- Learn to look at statistics
Advice - Look Around

- “Google” for your data, sometimes it is not that “deep” on the web
- Understand your enemies and keep up with current techniques
- Think outside the box
Thank You!

Alex Holden
aholden@holdsecurity.com